Rechtsgutachten zur elektronischen Datentreuhänderschaft

im Auftrag der

Telematikplattform für Medizinische Forschungsnetze (TMF)

Version 1.0

TMF-Produktnummer: P052011

A) Einleitung (Seiten A1 – A5)
Auszug aus dem Pflichtenheft zur Gutachtenvergabe

B) Gutachten (Seiten B1 – B82)
Gutachter: Prof. Dr. Dr. Christian Dierks, Dierks + Bohle Rechtsanwälte, Berlin
Reviewer: Prof. Dr. Alexander Roßnagel, Universität Kassel / Claus Burgardt, Anwaltskanzlei Sträter, Bonn

Hinweis: ein **Mustervertrag** für die Beauftragung eines Datentreuhänders ist als separates Dokument erhältlich (TMF-Produktnummer P052011).

Telematikplattform für Medizinische Forschungsnetze e. V., Neustädtische Kirchstr. 6, 10117 Berlin / Tel. 030 31011950 / info@tmf-ev.de

2 Anforderungen an das Rechtsgutachten zur elektronischen Datentreuhänderschaft

Die Datenschutzkonzepte der TMF sehen eine informationelle Gewaltenteilung vor, die durch eine Unabhängigkeit des administrativen Zugriffs auf verschiedene Komponenten und Anteile des Datenbestandes zu realisieren ist. Eine zentrale Komponente dieser verteilten Konzeption ist eine elektronisch geführte Patientenliste, die den Zusammenhang identifizierender Patientendaten (IDAT) zu Pseudonymen (PID) speichert. Eine treuhänderische Verwaltung dieser zentralen Patientenliste ist manchmal innerhalb eines Forschungsverbundes realisierbar, wenn ein Verbundteilnehmer unabhängig von den anderen diese Aufgabe übernimmt. In vielen Fällen werden aber an einen solchen Datentreuhänder erhöhte Anforderungen hinsichtlich eines Beschlagnahmeschutzes und auch hinsichtlich seiner Unabhängigkeit gestellt. Dies gilt z.B. für das in der TMF organisierte Kompetenznetz HIV/AIDS. Zusätzlich sehen sich kleinere oder nicht verteilt aufgestellte Forschungseinrichtungen oftmals nicht in der Lage, innerhalb ihrer Strukturen eine ausreichende administrative Unabhängigkeit für die Verwaltung einer solchen Patientenliste zu realisieren. Um das Konzept der informationellen Gewaltenteilung effektiv umzusetzen sind solche Forschungsorganisationen auf externe Partner angewiesen, die eine solche Treuhänderfunktion übernehmen können. Ein Treuhänder sollte ein rechtlich selbständig, unabhängiger, vertrauenswürdiger Dritter sein, bei dem die Daten auch rechtlich besonders durch ein Beschlagnahmeverbot und Zeugnisverweigerungsrecht geschützt sind.

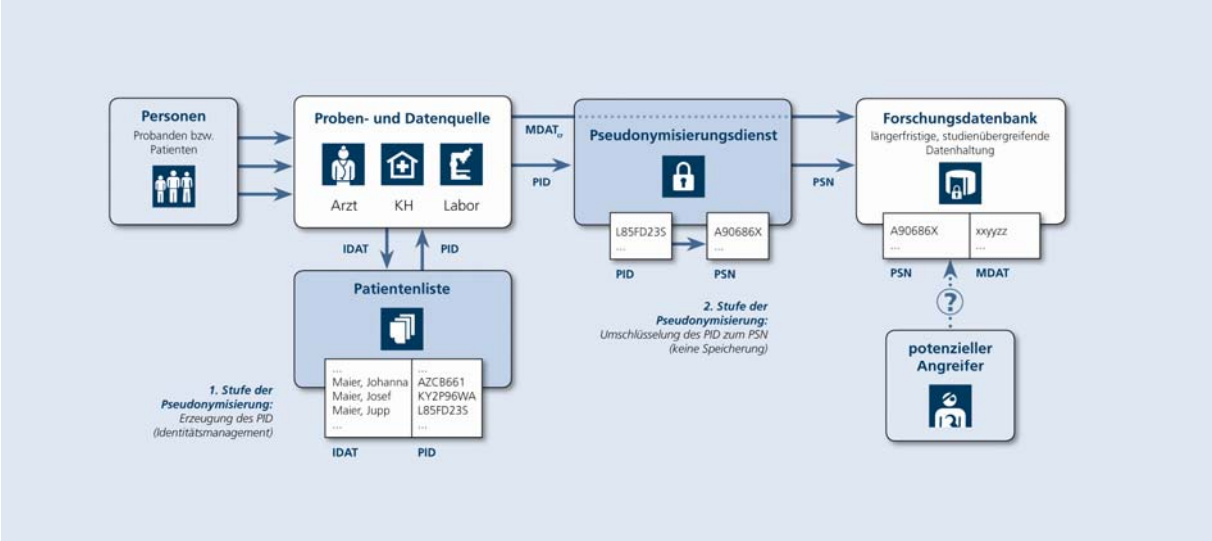
2.1 Beispiel der gewünschten Datenübermittlung

Um den geplanten Anwendungsfall zu verdeutlichen, sei hier der zukünftig gewünschte Ablauf der Verwaltung der Daten und deren Pseudonymisierung beschrieben:

Ein an einer klinischen Studie teilnehmender Patient sucht dazu einen Arzt (A1) eines Forschungsnetzes (Mitglied TMF) auf. Dieser gibt die identifizierenden Daten (IDAT) elektronisch an einen Treuhänder und erhält im Gegenzug umgehend ein Pseudonym (PID) zurück. Für den Arzt ist nicht zu erkennen, ob die identifizierenden Daten des Patienten bereits zuvor bei dem Treuhänder gespeichert wurden und das entsprechende Pseudonym bereits verwendet wird oder ob es erstmalig erstellt wurde. Alle Daten die im Verlauf der Studie von verschiedenen Ärzten und Forschern ermittelt werden, werden unter Verwendung des Pseudonyms verwaltet.

Sollte der Patient den behandelnden (Studien-)Arzt und Behandlungsort wechseln, könnte ein zweiter Arzt (A2) wiederum die identifizierenden Daten an den Treuhänder geben und das bereits verwendete Pseudonym erhalten. So ist sichergestellt, dass keine Dubletten entstehen und alle Daten eines Patienten unter einem Pseudonym verwaltet werden und so der Forschung zugänglich sind. Um eine längerfristige, studienübergreifende Datenhaltung zu ermöglichen sehen die Datenschutzkonzepte der TMF eine zusätzliche 2. Stufe der Pseudonymisierung vor. Eine möglicherweise notwendige Depseudonymisierung kann zudem ausschließlich von autorisierten Personen nach einem strengen Regelwerk durchgeführt werden.

Die zentrale Fragestellung an das hier zu erstellende Rechtsgutachten betrifft jedoch nur die Verwaltung der Patientenliste und damit die erste Stufe der Pseudonymisierung.



Datenschutzkonzept der TMF: Eine zweistufig verschlüsselte ID und die getrennte Haltung von Identifikationsdaten (IDAT) und medizinischen Daten (MDAT) sorgen für größtmögliche Sicherheit bei der Nutzung der Forschungsdatenbank. (PID = einfach verschlüsselter Patientenidentifikator, PSN = Pseudonym, zweifach verschlüsselter Patientenidentifikator)

2.2 Verwendungszweck, Ziele

Das Gutachten richtet sich in erster Linie an die TMF und ihre Mitgliedsverbünde, bzw. andere forschende medizinischen Einrichtungen, welche Patientenlisten und Datenbanken verwalten. Die TMF erwartet von dem Gutachten die notwendige Rechtssicherheit für das geplante Datentreuhändermodel. Sobald die rechtlichen Aspekte geklärt sind, wird ein Expertenteam die notwendige technische Infrastruktur für die Umsetzung des Datentreuhändermodels entwickeln.

Neben der Darstellung und Erörterung der relevanten rechtlichen Aspekte sollen auch Regeln und Leitlinien für die Datentreuhänderschaft erarbeitet und Musterverträge für die Beauftragung eines Datentreuhänders ausgearbeitet werden (Ausarbeitung eines Datentreuhändervertrages zwischen der TMF und einem Datentreuhänder bzw. zwischen einzelnen Forschungseinrichtungen und einem Datentreuhänder).

2.3 Inhaltliche Anforderungen

2.3.1 Beschlagnahmeschutz

Obwohl die Patientenliste nur die identifizierenden Daten und die entsprechenden Pseudonyme (und keine weiteren medizinischen Daten oder Forschungsergebnisse) enthält, haben die Patienten ein hohes Interesse daran, dass diese Liste nur von einem kleinen, definierten Personenkreis einsehbar ist. Insbesondere für mit dem HI Virus erkrankten Patienten ist die Verhinderung einer möglichen Verbreitung ihrer IDAT und der Tatsache ihrer Erkrankung entscheidend. Daher ist die Frage der Beschlagnahmesicherheit der Patientenliste eine der zentralen Fragen des Rechtsgutachtens.

Bekannt ist, dass die Beschlagnahme in § 97 StPO geregelt ist und der Sicherstellung von Gegenständen (hierzu zählen nach § 97 Abs. 5 StPO auch Datenträger) dient, die Beweismittel sind, aber nicht freiwillig herausgegeben werden. Nicht beschlagnahmt werden dürfen (vgl. § 97 Abs. 1 StPO) schriftliche Mitteilungen zwischen einem Beschuldigten (Patienten) und den Zeugnisverweigerungsberechtigten (Arzt), sowie Aufzeichnungen, welche Zeugnis-verweigerungsberechtigte über anvertraute Mitteilungen oder andere Umstände, auf die sich

das Zeugnisverweigerungsrecht erstreckt, gemacht haben (die gesamte Patientendokumentation unabhängig von der Aufzeichnungsart) andere Gegenstände einschließlich der ärztlichen Untersuchungsbefunde, auf die sich das Zeugnisverweigerungsrecht bezieht. Der Beschlagnahmeschutz gilt auch für Datenbestände, die für Datenabgleiche zur Täterauffindung geeignet wären (vgl. § 98b Abs. 1 StPO). Fraglich ist, ob ein solcher Datenbestand beispielsweise auch die Patientenliste sein könnte.

Der Beschlagnahmeschutz besteht nur, wenn ein Zeugnisverweigerungsrecht besteht und sich die zu beschlagnahmenden Gegenstände im Gewahrsam des Schweigepflichtigen oder des Krankenhauses befinden.

Problematisch ist hierbei zunächst, dass sich die Patientenliste auf einem Server bei einem Treuhänder befinden soll, sich somit also nicht im unmittelbaren Gewahrsam des Arztes befindet. Auch ein mittelbarer Gewahrsam liegt nicht zwangsläufig vor. Fraglich ist, ob und unter welchen Voraussetzungen ein als Treuhänder beauftragter IT-Dienstleister ein Dienstleister i.S.d. § 97 Abs. 2 S. 2 StPO sein kann. Sollte ein Beschlagnahmeschutz über diese Vorschrift nicht möglich sein, wären andere Möglichkeiten zu beleuchten. Könnte beispielsweise ein Notar als Treuhänder beauftragt werden, um einen Beschlagnahmeschutz zu erreichen? Welche Anforderungen würde das an den Gewahrsam, also die praktische Verwaltung und Zugriff auf die Patientenliste bzw. das Programm stellen? Neben der Gewahrsamproblematik stellen sich weitere Fragen zu § 97 StPO. Nicht alle Daten im Bereich medizinischer Forschung werden durch ärztliches Personal verarbeitet. Außerdem ist unklar, ob allein der Arzt-Status (eines ärztlichen Forschers, der nicht auch behandelnder Arzt der Betroffenen ist) bei Verarbeitung von personenbezogenen Patientendaten für Zwecke wissenschaftlicher Forschung das Beschlagnahmeverbot und das Zeugnisverweigerungsrecht zur Folge hat. Zur Verweigerung des Zeugnisses sind Ärzte nur über das berechtigt, "was ihnen in dieser Eigenschaft anvertraut worden oder bekanntgeworden ist" (§ 53 Abs. 1 Nr. 3 StPO). Auch die Sanktion der ärztlichen Schweigepflicht in § 203 StGB gilt für Ärzte nur, soweit ihnen Geheimnisse "als Arzt" anvertraut oder sonst bekanntgeworden sind. Fraglich ist daher, unter welchen Voraussetzungen die personenidentifizierenden Daten, die ein wissenschaftliches Institut zu Forschungszwecken erhalten hat, dortigen Ärzten "als Arzt" anvertraut oder bekanntgeworden sind. Können die IDat auch über die zeitliche Dauer der klinischen Studie in der Patientenliste verwaltet werden oder gilt der Beschlagnahmeschutz nur für die Dauer der Behandlung? Wer muss mit der Treuhänderschaft beauftragt werden, um einen maximalen Beschlagnahmeschutz zu erreichen? Kann dies ein unabhängiger Dienstleister (iSd § 97 StPO?) sein, der über die entsprechende Hardwareausrüstung verfügt (z.B. eine Firma wie IBM)?

Die einzelnen Fragen stellen sich wie folgt:

F.2.1 Wer ist "Dienstleister, der für die Genannten personenbezogene Daten erhebt" i.S.d. §97 Abs. 2 S. 2 StPO? Gilt auch der Dienstleister des Dienstleisters als Dienstleister iSd § 97 StPO? Gibt es hierzu bereits Kommentierungen bzw. Auslegungshilfen?

F.2.2 Wenn ein Beschlagnahmeschutz über einen Dienstleister nicht erreicht werden kann, wäre dies über einen zugelassenen Notar als der Treuhänder möglich? Welche Anforderungen stellt der von § 97 StPO geforderte (Mit-)Gewahrsam an die Verwaltung und Herausgabe von Daten? Setzt § 97 StPO voraus, das sich der Server auf dem die Patientenliste liegt in den Räumlichkeiten des Notars befindet, oder könnte der Notar ein Rechenzentrum mit der Verwahrung der Patientenliste beauftragen? Wer darf auf die Patientenliste Zugriff haben ohne den Beschlagnahmeschutz zu gefährden?

F.2.3 Die Systematik und der Umfang des erreichbaren Beschlagnahmeschutzes ist zu beschreiben

F.2.4 Was ist "Untersuchung" iSd § 53 StPO? Ist auch der forschende Arzt, Arzt iSd § 53 StPO?

F.2.5 Wie weitgehend ist ein Beschlagnahmeschutz für die Daten einer zentralen Patientenliste erreichbar, wenn diese zumindest teilweise Daten außerhalb eines Behandlungskontextes enthält? Besteht der Beschlagnahmeschutz für die Patientenliste über die zeitliche Dauer der Behandlung? Hintergrund ist der Wunsch, dass die gewonnen medizinischen Daten der Forschung längerfristig zur Verfügung stehen. Entsprechend langfristig und unabhängig von der Dauer der klinischen Studie, sollte auch die Speicherung der identifizierenden Daten des Patienten möglich sein.

F.2.6 Ist der erreichbare Beschlagnahmeschutz davon abhängig, wer einen Datentreuhänder beauftragt? Hintergrund ist der Wunsch, dass die TMF den Datentreuhänder für ihre Mitgliedsverbünde beauftragt.

F.2.7 Welche besonderen rechtlichen Konsequenzen für oder Anforderungen an einen Datentreuhänder ergeben sich, wenn dieser mehrere Patientenlisten für unterschiedliche Mandanten bzw. Forschungseinrichtungen verwaltet? Hat es auf den Beschlagnahmeschutz der Daten Einfluss, ob ein zentraler Datentreuhänder oder mehrere dezentrale Datentreuhänder (z.B. eine zentrale Stelle für jede größere Stadt) existieren?

F.2.8 Gibt es Verwendungseinschränkungen für rechtmäßig beschlagnahmte Daten (z.B. bei der Ermittlung gegen einen Arzt)? Sind die so beschlagnahmten Daten mögliche Beweismittel gegen andere Beschuldigte/andere Straftaten wie z.B. Körperverletzung durch einen HIV-Patienten? Muss aus § 108 II StPO gefolgert werden, dass ein Verwertungsverbot nur für Strafverfahren gegen Patientinnen wegen einer Straftat nach § 218 StGB besteht?

2.4 Anforderungen aufgrund des Arzneimittelgesetzes (AMG)

F.2.9 Welche besonderen rechtlichen Konsequenzen für oder Anforderungen an einen Datentreuhänder ergeben sich, wenn dieser Patientenlisten für Studien verwaltet, die den Auflagen des Arzneimittelgesetzes (AMG) unterliegen?

2.5 Datenschutz

F.2.10 Welche Anforderungen werden an einen Dienstleister grundsätzlich und an sein administratives Personal (Wartungstechniker) bezüglich Ausbildung und Schweigepflicht gestellt und wie überprüft? Wie kann die Vertraulichkeit eines Dienstleisters gewährleistet werden?

F.2.11 Wo verbleiben die gespeicherten Daten, falls die Finanzierung des Datentreuhänders nicht weiter gewährleistet ist.

2.6 Auskunft, Sicherung und Haftung und Sonstiges

F.2.12 Welche Auskunftspflichten gelten für einen Datentreuhänder gegenüber dem Auftraggeber und gegenüber Patienten, die in die Patientenliste eingeschlossen sind? Sind diese abhängig von einer Patienteneinverständniserklärung?

F.2.13 Welche Regelungen sind zur Sicherung einer dauerhaften Verfügbarkeit der Daten für den Auftraggeber zwischen Auftraggeber (TMF bzw. Kompetenznetz/Arzt) und Auftragnehmer (Treuhänder) zu treffen? (Datensicherheit, Backup, Ausfallsicherheit etc.)

F.2.14 Welche Schadenersatzregelungen sollten für den Fall einer Nichtverfügbarkeit der Daten getroffen werden? Wie ist Schadensersatz und Haftung bei z.B. Datenverlust sichergestellt? Ist eine Versicherung möglich?

F.2.15 Wie ist der Zugriffsschutz auf z.B. Sicherungsbänder durchzuführen?

F.2.16 Welche Haftungsregelungen gelten für einen Datentreuhänder?

F.2.17 Gibt es weitere rechtliche Rahmenbedingungen, welche für den Datentreuhänder relevant sind und hier noch nicht berücksichtigt wurden?

F.2.18 Auflistung von Regeln und Leitlinien für die Datentreuhänderschaft

F.2.19 Ausarbeitung eines Datentreuhändervertrages (zwischen TMF und Datentreuhänder)

Dieser Fragenkatalog ist nicht abschließend. Sollten sich während der Erarbeitung des Gutachtens weitere Fragen ergeben und/oder andere wichtige Bereiche in diesem Katalog nicht aufgeführt worden sein, wird um entsprechenden Hinweis bzw. entsprechende Bearbeitung gebeten.

Gutachten

Rechtsgutachten zur elektronischen Datentreuhänderschaft

DIERKS + BOHLE
RECHTSANWÄLTE

<Version 1.1 – 06.02.2008>

TMF

Inhaltsverzeichnis

Wir gehen bei Beantwortung der Fragen davon aus, dass vor der Weiterleitung patientenbezogener Daten an den Dienstleister in jedem Einzelfall eine Einwilligung des Patienten bzw. Probanden vorliegt. In strafrechtlicher Hinsicht ist dies im Hinblick § 203 StGB von Bedeutung, weil das unbefugte Offenbaren patientenbezogener Daten durch einen Arzt an einen externen Dienstleister eine Verletzung von Privatgeheimnissen gemäß § 203 Abs. 1 Nr. 1 StGB darstellen kann. Anderes gilt nur, wenn der Dienstleister selbst als Gehilfe des Berufsgeheimnisträgers iSd § 203 Abs. 3 StGB in den Bereich der Befugnisinhaber fiele und so zum Bereich der Geheimnisträger gehörte. In der vorliegenden Konstellation bestehen hierfür allerdings keine ausreichenden Anhaltspunkte (vgl. 2.7.), so dass die Einholung einer Einwilligung des Patienten bzw. Probanden aus strafrechtlicher Sicht dringend anzuraten ist.

F2.1 Wer ist „Dienstleister, der für die Genannten personenbezogene Daten erhebt“ iSd § 97 Abs. 2 Satz 2 StPO? Gilt auch der Dienstleister des Dienstleisters als Dienstleister iSd § 97 Abs. 2 Satz 2 StPO? Gibt es hierzu bereits Kommentierungen bzw. Auslegungshilfen?

Nachfolgend soll nicht nur eine Definition des Dienstleisters gegeben werden, sondern im Hinblick auf die Frage 2.2. auch geprüft werden, ob über einen Dienstleister ein wirksamer Beschlagnahmeschutz der bei einem Dienstleister zu verwaltenden Patientenliste erreicht werden kann. Die Ausführungen zu 2.3. (Die Systematik und der Umfang des erreichbaren Beschlagnahmeschutzes sind zu beschreiben) werden daher in die Beantwortung dieser Frage eingebunden.

2.1.1 Der Dienstleister im Zusammenhang mit der Einführung der elektronischen Gesundheitskarte

Der Begriff des Dienstleisters hat erst mit der Ergänzung des § 97 Abs. 2 StPO durch das „Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz – GMG)“ vom 14.11.2003 Eingang in § 97 Abs. 2 Satz 2 StPO gefunden.[1] Seither unterliegen gemäß § 97 Abs. 2 Satz 2 StPO auch solche Gegenstände nicht der Beschlagnahme,

> „auf die sich **das Zeugnisverweigerungsrecht der Ärzte** (...) **erstreckt**, wenn sie im Gewahrsam einer Krankenanstalt oder eines **Dienstleisters, der für die Genannten personenbezogene Daten erhebt, verarbeitet oder nutzt**, sind (...).“ (§ 97 Abs. 2 Satz 2 StPO, Hervorhebungen durch die Verfasser)

Durch diese Gesetzesänderung wurde der Kreis der nicht der Beschlagnahme unterliegenden Gegenstände insoweit erweitert, als die Anbindung des Beschlagnahmeverbotes an den Gewahrsam eines Berufsgeheimnisträgers gelockert wurde. So ist zum einen bereits in § 97 Abs. 2 Satz 1 StPO der Anwendungsbereich des Beschlagnahmeverbotes ausdrücklich auf die im Besitz des Patienten befindliche Gesundheitskarte im Sinne des § 291a des Fünften Buches Sozialgesetzbuch (SGB V) erweitert worden.[2] Zum zweiten werden nunmehr gemäß § 97 Abs. 2 Satz 2 StPO auch Gegenstände vor einer Beschlagnahme geschützt, die sich weder im Gewahrsam der Patienten noch dem eines zeugnisverweigerungsberechtigten Arztes, sondern im Gewahrsam eines Dienstleisters befinden, der für den Zeugnisverweigerungsberechtigten Daten erhebt, verarbeitet oder nutzt. Nach der Gesetzesbegründung stehen diese Ergänzungen im Zusammenhang mit der Einführung der elektronischen[3] Gesundheitskarte.[4]

Durch den Gesetzgeber sind die mit der Einführung der Gesundheitskarte verbundenen Risiken für das geschützte Arzt-Patienten-Verhältnis erkannt und berücksichtigt worden.[5] Denn infolge der Einführung der Gesundheitskarte befinden sich sensible Gesundheitsdaten nicht mehr nur im Gewahrsam eines zeugnisverweigerungsberechtigten Arztes, sondern infolge der Speicherung auf der im Patientengewahrsam befindlichen Karte auch in der Hand des Patienten:

> „Bislang befinden sich Gesundheitsdaten in der Regel im Gewahrsam zeugnisverweigerungsberechtigter Ärzte und unterliegen damit dem Beschlagnahmeschutz. Mit der Einführung der elektronischen Gesundheitskarte werden Gesundheitsdaten in erheblichem Umfang auch in der Hand der Patienten sein. Die damit beabsichtigten Qualitätsverbesserungen im Gesundheitswesen dürfen nicht zu einer Verschlechterung der Rechtsstellung der Patienten führen. Sie müssen darauf vertrauen können, dass die auf der Gesundheitskarte befindlichen Daten tatsächlich nur für den mit der Gesundheitskarte beabsichtigten Zweck, der Optimierung ihrer Behandlung, verwendet werden.“[6]

Die Erweiterung des Beschlagnahmeschutzes auf die Gesundheitskarte und die darauf gespeicherten Daten durch den Gesetzgeber (vgl. § 97 Abs. 2 Satz 1 StPO) war daher konsequent.

---

[1] BGBl. 2003 I S. 2190.

[2] Vgl. Bales/Dierks/Holland/Müller, Die elektronische Gesundheitskarte, 2007, § 97 B III, S. 168 ff.

[3] In der BT-Drs. 16/5846, 38, wird klargestellt, dass mit der in § 97 Abs. 2 Satz 2 StPO Bezug genommenen „Gesundheitskarte“ die elektronische Gesundheitskarte gemeint ist.

[4] BT-Drs. 15/1525.

[5] BT-Drs. 15/1525, S. 167.

[6] BT-Drs. 15/1525, S. 167.

In dem GKV-Modernisierungsgesetz ist zur Wahrung des Vertrauensverhältnisses zwischen Arzt und Patienten einer weiteren, insbesondere im Hinblick auf die Gesundheitskarte bestehenden Besonderheit Rechnung getragen worden. Nach § 97 Abs. 2 Satz 2 StPO wird der Beschlagnahmeschutz nunmehr auch auf Dienstleister erweitert, die die im Zuge der Einführung der Gesundheitskarte erforderliche technische Infrastruktur stellen und räumlich sowohl vom Zeugnisverweigerungsberechtigten wie auch vom Patienten getrennt sind:

> „Gleiches gilt, wenn zur Erreichung der vorgenannten Ziele Dienstleister in Anspruch genommen werden, die Daten der Versicherten zur Verbesserung von sektorübergreifenden Behandlungen unabhängig von einzelnen Behandlungseinrichtungen dokumentieren und für die weitere Versorgung zur Verfügung stellen.“[7]

Zum Begriff des „Dienstleisters“ kann als gesichert gelten, dass hierzu im Sinne des § 97 Abs. 2 Satz 2 StPO jedenfalls solche Personen und Unternehmen zu zählen sind, die im Zuge der Einführung und Verwendung der elektronischen Gesundheitskarte (§ 291a SGB V) notwendiger Bestandteil der technischen Infrastruktur sind, indem sie Patienteninformationen erheben, verarbeiten oder nutzen. Nicht der Beschlagnahme unterliegen damit auf Servern gespeicherte Daten, auf die mittels der elektronischen Gesundheitskarte zugegriffen werden kann, und die sich im Gewahrsam eines Dienstleisters befinden.[8]

2.1.2 Der Dienstleister im Sinne des Gesetzeswortlautes

Zu klären und für die uns vorgelegte Fragestellung von Bedeutung ist indes, ob der Dienstleisterbegriff des § 97 Abs. 2 StPO tatsächlich auf den Zusammenhang mit der elektronischen Gesundheitskarte zu beschränken ist oder ob ausgehend vom Wortlaut des § 97 Abs. 2 Satz 2 StPO sowie aufgrund der fortgeschrittenen Bedeutung der Telematik im Medizinwesen, der der Gesetzgeber bei der Einführung der elektronischen Gesundheitskarte offenkundig Rechnung tragen wollte und getragen hat, von einem umfassenderen Verständnis des Dienstleisterbegriffs auszugehen ist.

Letzteres ist bereits aufgrund des Gesetzeswortlautes naheliegend. Aus unserer Sicht ist der Dienstleisterbegriff weit zu verstehen und über den Zusammenhang mit der technischen Infrastruktur der elektronischen Gesundheitskarte hinausreichend. Es wird in § 97 Abs. 2 Satz 2 StPO lediglich von Dienstleistern gesprochen, die für die Zeugnisverweigerungberechtigten

[7] BT-Drs. 15/1525, S. 168.

[8] Bales/Dierks/Holland/Müller, Die elektronische Gesundheitskarte, 2007, § 97 B III, Rdnr. 7.

personenbezogene Daten erheben, verarbeiten oder nutzen. Eine Einschränkung des Dienstleisterbegriffs auf die im Rahmen der technischen Infrastruktur für die elektronische Gesundheitskarte erforderlichen Dienstleister kann dem Wortlaut des § 97 Abs. 2 Satz 2 StPO nicht entnommen werden. Diese Sichtweise wird dadurch unterstützt, dass der Begriff des Dienstleisters in § 97 Abs. 2 Satz 2 StPO keinen konkreten Bezug zur elektronischen Gesundheitskarte in § 97 Abs. 2 Satz 1 StPO aufweist. Die elektronische Gesundheitskarte ist gemäß § 97 Abs. 2 Satz 1 StPO ausdrücklich als Ausnahme eines Gegenstandes aufgeführt, der nicht beschlagnahmefähig ist, obgleich sich dieser regelmäßig nicht im Gewahrsam des zur Zeugnisverweigerung Berechtigten befindet.[9] § 97 Abs. 2 Satz 2 StPO erweitert hingegen den Beschlagnahmeschutz allgemein u.a. auf personenbezogene Patientendaten erhebende, verarbeitende und nutzende Dienstleister. Vor der Ergänzung des § 97 Abs. 2 Satz 2 StPO war die Beschlagnahmefreiheit von Datenträgern nicht gesichert, wenn sie von einem Dienstleister außerhalb des Gewahrsams des Zeugnisverweigerungsberechtigten aufbewahrt wurden.[10]

Aus der Gesetzesbegründung ergibt sich nichts Abweichendes. Ausweislich dieser sollen Dienstleister zum Zwecke von Qualitätsverbesserungen im Gesundheitswesen in Anspruch genommen werden können, um Daten der Versicherten zur Verbesserung von sektorübergreifenden Behandlungen unabhängig von einzelnen Behandlungseinrichtungen zu dokumentieren und für die weitere Versorgung zur Verfügung zu stellen, wobei es nicht zu einer Verschlechterung der Rechtsstellung der Patienten kommen soll.[11] Eine Beschränkung des Dienstleisterbegriffs auf die elektronische Gesundheitskarte lässt sich der Gesetzesbegründung nicht entnehmen.

Zwar mag die Einfügung des „Dienstleister“-Begriffs in § 97 Abs. 2 StPO mit der elektronischen Gesundheitskarte als Anlass verknüpft sein. Der Gesetzgeber hat bei der Wahl der gesetzlichen Formulierung jedoch einen umfassenderen Zweckbezug hergestellt, namentlich allgemein die Erhebung personenbezogener Daten im Auftrag der Zeugnisverweigerungsberechtigten. Auch die vom Gesetzgeber angeführten Ziele bei der Anerkennung des Beschlagnahmeschutzes bei Dienstleistern sind allgemein formuliert; der Gesetzgeber führt insoweit die Qualitätsverbesserung in der Krankenbehandlung, erhöhte Transparenz im Gesundheitswesen, Stärkung der

[9] Bales/Dierks/Holland/Müller, Die elektronische Gesundheitskarte, 2007, § 97 B III, Rdnr. 3.

[10] Dierks/Nitz/Grau, Gesundheitstelematik und Recht, 2003, S. 164; Reng/Debold/Specker/ Pommerening, Generische Lösungen zum Datenschutz für die Forschungsnetzwerke in der Medizin, 2006, S. 38.

[11] BT-Drs. 15/1525, S. 168.

Patientensouveränität[12] und Kosteneinsparungen[13] an. Diese Ziele sollen sich durch die Einführung der elektronischen Gesundheitskarte erreichen lassen, sie sind aber nicht darauf beschränkt.

Dem hier vertretenen weiten Verständnis des Dienstleisterbegriffs folgen auch Vertreter in der medizinrechtlichen Literatur. Diese gehen davon aus, dass der Dienstleisterbegriff nicht auf den in der Gesetzesbegründung angeführten Zusammenhang mit der Einführung der elektronischen Gesundheitskarte zu beschränken ist, sondern grundsätzlich dem Einsatz der Telematik im Medizinwesen und den sich daraus ergebenden besonderen Anforderungen für den Schutz des Arzt-Patienten-Verhältnisses Rechnung getragen werden sollte.[14] So vertreten Bales/Dierks/Holland/Müller in der Kommentierung zur elektronischen Gesundheitskarte, dass grundsätzlich Daten im Gewahrsam eines Dienstleisters, der für die Zeugnisverweigerungsberechtigten personenbezogene Daten erhebt, verarbeitet oder nutzt, der Beschlagnahme entzogen sind. Als beschlagnahmefreie Gegenstände sollen ausdrücklich auch einrichtungsübergreifende elektronische Krankenakten erfasst sein, bei denen Serviceeinrichtungen die Daten einrichtungsübergreifend verwalten.[15] Auch Hornung vertritt einen umfassenden Begriff des Dienstleisters im Zusammenhang mit der Einführung der elektronischen Gesundheitskarte.[16]

Für die Auffassung, dass durch die Einführung des allgemein formulierten Dienstleisterbegriffs in den § 97 Abs. 2 Satz 2 StPO grundlegend der Bedeutung der Telematik im Gesundheitswesen[17] Rechnung getragen werden sollte, lässt sich auch anführen, dass dies in der medizinrechtlichen Literatur und auch von Datenschützern schon seit Längerem und nicht nur im Zusammenhang mit der Einführung der elektronischen Gesundheitskarte gefordert worden ist.[18] Nach den entsprechenden Forderungen sollten Dienstleister bzw. datenverarbeitende Stellen in den § 97

[12] BT-Drs. 15/1525, S. 143f; siehe auch: Kranig in Hauck/Noftz, SGB V (Erg.-Lfg. 1/07), § 291 Rn. 29 .

[13] Dies betont: Weichert, DuD 2004, S. 391.

[14] Bales/Dierks/Holland/Müller, Die elektronische Gesundheitskarte, 2007, § 97 B III, Rdnr. 6.

[15] Bales/Dierks/Holland/Müller, Die elektronische Gesundheitskarte, 2007, § 97 B III, Rdnr. 6.

[16] Hornung, Die digitale Identität, 2005, S. 235.

[17] Vgl. dazu eingehend: Dierks/Nitz/Grau, Gesundheitstelematik und Recht, 2003.

[18] Dierks/Nitz/Grau, Gesundheitstelematik und Recht, 2003, S. 164 mit Hinweis auf: Thüringer Landesbeauftragte für den Datenschutz, 3. Tätigkeitsbericht 1999, S. 165 f.; Der Bayerische Landesbeauftragte für den Datenschutz, 16. Tätigkeitsbericht, 1994 sowie die Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken.

Abs. 2 Satz 2 StPO aufgenommen werden[19], um den Beschlagnahmeschutz von Patientendaten an die tatsächlichen technischen Gegebenheiten im Bereich der Telematik anzupassen.[20]

Auch jenseits des Wortlautes der Vorschrift spricht daher vieles dafür, dass Anlass für die Änderung des § 97 Abs. 2 Satz 2 StPO zwar die Einführung der elektronischen Gesundheitskarte gewesen sein mag, die Gesetzesänderung aber auch insgesamt den veränderten Gegebenheiten in den Arzt-Patienten-Verhältnissen durch den Einsatz der Telematik Rechnung getragen werden sollte. Denn diese beschränkt sich nicht auf die Schaffung der technischen Infrastruktur für die Einführung der elektronischen Gesundheitskarte.

Allerdings weisen wir darauf hin, dass hierzu in der strafgerichtlichen Rechtsprechung und der strafrechtlichen Literatur bislang keine nähere Auseinandersetzung stattgefunden hat, weshalb von einer gefestigten Meinung nicht gesprochen werden kann. Die strafgerichtliche Rechtsprechung hatte sich – soweit ersichtlich – noch nicht zum vergleichsweise neuen Dienstleisterbegriff des § 97 Abs. 2 Satz 2 StPO zu äußern.

In der strafrechtlichen Literatur finden sich bislang nur vereinzelt Hinweise auf den Dienstleisterbegriff. Die Standardkommentare zur Strafprozessordnung schweigen zum Dienstleisterbegriff.[21] Soweit ersichtlich, hat sich in der strafprozessualen Kommentarliteratur

---

[19] Vgl.: Dierks/Nitz/Grau, Gesundheitstelematik und Recht, 2003, S. 167: § 97 Abs. 2 Satz 2 StPO sollte wie folgt ergänzt werden: „Der Beschlagnahme unterliegen auch nicht Gegenstände, auf die sich das Zeugnisverweigerungsrecht der Ärzte (...) erstreckt, wenn sie im Gewahrsam einer Krankenanstalt oder einer Stelle zur Auftragsdatenverarbeitung sind, (...)“. Betrachtet und vergleicht man den gesetzgeberischen Vorschlag aus der medizinrechtlichen Literatur, so ist ein qualitativer Unterschied zwischen der „Stelle zur Auftragsdatenverarbeitung“ und dem „Dienstleister, der für die Genannten personenbezogene Daten erhebt, verarbeitet oder nutzt,“ (§ 97 Abs. 2 Satz 2 StPO) nicht zu erkennen. Insoweit auch erhellend: Bales/Dierks/Holland/Müller, Die elektronische Gesundheitskarte, 2007, § 97 B III, Rdnr. 6, die vom „Dienstleister im Wege der Auftragsdatenverarbeitung“ sprechen.

[20] Es wurde vorgeschlagen, den Gewahrsamsbegriff in § 97 Abs. 2 Satz 1 StPO insofern nicht als tatsächliche Sachherrschaft, sondern als tatsächliche Zugriffsmöglichkeit zu begreifen. Die Sachbezogenheit des Beschlagnahmeschutzes führe im Bereich der Telematik zu Wertungswidersprüchen, weil die tatsächliche Sachherrschaft über das Speichermedium nichts über die Zugriffsmöglichkeit von außen auf elektronischem Wege aussagt. Durch den Einsatz der Telematik verliere das Kriterium des Gewahrsams an Bedeutung für die Identifikation der Schutzwürdigkeit personenbezogener Gesundheitsdaten (Dierks/Nitz/Grau, Gesundheitstelematik und Recht, 2003, S. 167).

[21] Vgl. etwa: Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97; Nack in Karlsruher Kommentar zur StPO, 5. Aufl., § 97; Schäfer in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 97 Rdnr. 118, § 97; Rudolphi in Systematischer Kommentar zur StPO, 10. Aufbau/Erg.Lfg., § 97.

bislang nur Löffelmann zum Dienstleister geäußert, der das Beschlagnahmeverbot auf Gegenstände im Gewahrsam (lediglich) auf „Abrechnungsstellen“ erstreckt.[22] Bisher war es nahezu einhellige Meinung, dass die Abrechnungsstelle nicht unter den Begriff der Krankenanstalt im Sinne des § 97 Abs. 2 Satz 2 StPO fällt und ein Beschlagnahmeverbot dort nicht besteht.[23]

Doch allein die Abrechnungsstelle als Dienstleister gemäß § 97 Abs. 2 Satz 2 StPO zu bezeichnen, greift zu kurz. Dies ergibt sich bereits aus der technischen Ausgestaltung der Gesundheitskarte. Denn nur ein sehr geringer Teil der Daten kann auf der Karte selbst gespeichert werden. Der weitaus größere Teil, insbesondere die elektronische Krankenakte als freiwillige Anwendung, wird voraussichtlich auf Servern gespeichert werden.[24] Die elektronische Gesundheitskarte dient dann nur als Schlüssel, um an die dort gespeicherten Daten zu gelangen. Schützt man nun die Gesundheitskarte durch ein Beschlagnahmeverbot nach § 97 Abs. 2 Satz 1 StPO, so müssen konsequenterweise auch Daten, die technisch nicht auf der Karte gespeichert werden können, jedoch mit den Daten auf der Karte eine Einheit darstellen, effektiv geschützt werden. Speicherort dieser Daten sind von Dritten betriebene Server, auf die Ärzte, Krankenhäuser und Krankenkassen bei Bedarf zugreifen können und sollen. Daher sind auch die Betreiber solcher Datenbankserver jedenfalls als Dienstleister i.S.d. § 97 Abs. 2 Satz 2 StPO zu betrachten.[25]

Der Dienstleister im medizinischen Forschungsverbund

Kann der Begriff des Dienstleisters hiernach grundsätzlich durchaus weiter verstanden werden, stellt sich die Frage, ob auch der Dienstleister eines medizinischen Forschungsverbundes unter den Dienstleisterbegriff des § 97 StPO subsumiert werden kann.

An der Begründung eines Beschlagnahmeschutzes bestehen in der uns zur Begutachtung vorgegebenen Konstellation Zweifel. Diese gehen in erster Linie auf den Umstand zurück, dass die Patientenliste (hauptsächlich) medizinischen Forschungszwecken dienen soll und die Datenübermittlung, -speicherung und -nutzung durch den Dienstleister keinen klar erkennbaren und intendierten (Rück)Bezug zu demjenigen Arzt-Patienten-Verhältnis besitzen, aus dem die Daten stammen.

---

[22] Krekeler/Löffelmann, AnwaltKommentar StPO, § 97 Rdnr. 10.

[23] Vgl. Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97 Rdnr. 14; Nack in Karlsruher Kommentar zur StPO, 5. Aufl., § 97 Rdnr. 21; Schäfer in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 97 Rdnr. 118.

[24] Vgl. Weichert, DuD 2004, S. 391 (394); Holland/Bales, GesR 2005, S. 299, 303; Hornung, Die digitale Identität, S. 213 ff.

[25] So auch Hornung, Die digitale Identität, 2005, S. 234 f.

Zwar kann auch die ärztliche Berufsausübung in Form der Erhebung von Daten zu Forschungszwecken (vgl. unten 2.4.) im Grundsatz ein gemäß § 53 StPO geschütztes Vertrauensverhältnis zwischen Arzt und Patient bzw. Proband und daran anknüpfend einen Beschlagnahmeschutz für Beweismittel im Gewahrsam des zeugnisverweigerungsberechtigten Arztes iSd § 97 StPO begründen. Dies gilt jedoch nicht in allen Fällen; vielmehr müssen im Licht des Normzwecks der §§ 53 und 97 StPO spezifische Anforderungen erfüllt sein, damit das Beschlagnahmeprivileg Geltung entfaltet.

Schutzgut des § 53 StPO ist das Vertrauens- bzw. Kommunikationsverhältnis zwischen dem zeugnisverweigerungsberechtigten Berufsangehörigen und denen, die deren Hilfe und Sachkunde in Anspruch nehmen.[26] Um ein solches (geschütztes) Vertrauensverhältnis handelt es sich bei jeder freiwilligen Hilfe und Inanspruchnahme ärztlicher Hilfe und Sachkunde.[27] Wer sich in ärztliche Behandlung und Beratung begibt, muss und darf erwarten, dass alles, was der Arzt im Rahmen seiner Berufsausübung im Zusammenhang mit dem Patienten erfährt, geheim bleibt und nicht zur Kenntnis Unberufener gelangt. Diese Vertraulichkeit ist Voraussetzung für die Bildung des Vertrauens, das zu den Grundvoraussetzungen ärztlichen Wirkens, zu dem auch die forschende Tätigkeit gehört, zählt.[28] An dieses geschützte Vertrauensverhältnis anknüpfend sind gemäß § 97 Abs. 1 StPO schriftliche Mitteilungen zwischen Beschuldigtem und Arzt, Aufzeichnungen, die vom Arzt über den Beschuldigten gemacht wurden und dem Zeugnisverweigerungsrecht unterliegen und ärztliche Untersuchungsbefunde, auf die sich das Zeugnisverweigerungsrecht erstreckt, beschlagnahmefrei. § 97 Abs. 1 StPO verhindert so eine Umgehung des Zeugnisverweigerungsrechtes durch Beschlagnahme des Papier gewordenen Wortes und sichert den Schutzzweck des Zeugnisverweigerungsrechtes: die geschützte Kommunikation zwischen Arzt und Patienten bzw. Probanden („Was der Mund nicht zu offenbaren braucht, darf auch der Hand nicht entrissen werden.“).

Die geschützte Sphäre des Arzt-Patienten-Verhältnisses findet indes nach dem gesetzlichen Grundansatz ihre Grenze, wenn Daten zur weiteren Speicherung und Nutzung an eine externe Stelle übertragen werden. Daten aus dem Arzt-Patienten-Verhältnis bleiben grundsätzlich nur dann vor staatlichem Zugriff geschützt, solange sie sich im Gewahrsam des zeugnisverweigerungsberechtigten Arztes befinden. Nur diese Sphäre schützt auch § 97 StPO.[29] Werden die vom behandelnden Arzt erhobenen Daten an außerhalb seiner Gewahrsamssphäre

[26] Vgl. BGH, Urteil vom 20.02.1985 – 2 StR 561/84.

[27] LG Stuttgart, Beschl. vom 17.03.1994 – 5 Ls 1248/93.

[28] BVerfG NJW 1972, 1123, 1124; Narr, Ärztliches Berufsrecht, 13. Erg-Lfg., B 266.

[29] Schäfer in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 97, Rdnr. 27.

stehende Stellen übertragen, die selbst nicht der ärztlichen Schweigepflicht unterliegen, entfällt der Beschlagnahmeschutz.[30]

Nur ausnahmsweise erfolgt gemäß § 97 Abs. 2 Satz 2 StPO eine Erweiterung des Beschlagnahmeschutzes, namentlich in den Fällen, in denen sich die Beweismittel im Gewahrsam eines Dienstleisters befinden, der „für den Zeugnisverweigerungsberechtigten“ personenbezogene Daten erhebt, verarbeitet oder nutzt. Mit dieser Formulierung stellt das Gesetz ersichtlich einen Bezug der Tätigkeit des Dienstleisters zu dem Zeugnisverweigerungsberechtigten und damit zu dem das Zeugnisverweigerungsrecht begründenden konkreten Vertrauensverhältnis zwischen Arzt und Patient her. Dies ist unter Berücksichtigung des Schutzzwecks der Zeugnisverweigerungsrechte nach § 53 StPO vorgezeichnet und führt dazu, dass das Beschlagnahmeverbot nur dann eingreifen kann, wenn die dem Dienstleister zur Bearbeitung übermittelten Daten zu dem spezifischen Arzt-Patienten-Verhältnis, aus dem sie stammen, einen unmittelbaren (Rück)Bezug besitzen.

Die „bloße“ Generierung von Daten aus einem Arzt-Patienten-Verhältnis und deren vom Behandlungskontext losgelöste Weiterverwendung außerhalb der Gewahrsamssphäre des Arztes zu Forschungszwecken ohne Bezug zu dem jeweiligen Patienten weisen nicht den für den Schutz des Vertrauensverhältnisses notwendigen personalen Bezug zu den an diesem Vertrauensverhältnis Beteiligten auf und genügen daher nicht für die Begründung eines Beschlagnahmeverbotes.[31]

---

[30] Insbesondere von Seiten der Datenschützer wird daher gefordert, dass vor dem Hintergrund verschiedener Konstellationen in der Praxis, in denen Patientendaten außerhalb der geschützten Räume des Arztes oder ärztlicher Einrichtungen verarbeitet werden (z.B. externe Mikroverfilmung, externe Archivierung, Vergabe von Schreibarbeiten an externe Schreibbüros, Einschaltung externer Inkassounternehmen usw.) der Beschlagnahmeschutz in sachgerechter Weise ausgedehnt wird. Diese Forderung stand auch im Zusammenhang mit der Entwicklung von Gesundheitsnetzen verschiedener öffentlicher und privater Stellen, die durch die anonymisierte Vernetzung von Patienten- und Arztdaten die schnelle Verfügbarkeit von Informationen zur Verbesserung der Qualität der ärztlichen Behandlung durch moderne Kommunikationsverfahren sicherstellen sollten (vgl. LfD Saarland 17. Tätigkeitsbericht (1997 / 98), 11/1926, 11.2.).

[31] Nicht zuletzt deshalb fordern Datenschützer und Verbände seit langem, und auch nach der Novelle des § 97 Abs. 2 StPO[31] den Gesetzgeber auf, ein sog. *Forschungsgeheimnis für medizinische Daten*, d.h. des Schutzes von Patientendaten außerhalb des Gewahrsams eines behandelnden (Studien-) Arztes zu Forschungszwecken, anzuerkennen und in den Schutzkatalog der §§ 53 f., 97 StPO, § 203 StGB zu integrieren, um auch in diesem Bereich Daten- und Rechtssicherheit zu erlangen. (Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004: „Mit der Übermittlung verlieren die Daten aber regelmäßig den strafrechtlichen Schutz vor Offenbarung und den

Auf diesen maßgeblichen Zusammenhang zwischen den an einen Dienstleister aus dem geschützten Arzt-Patienten-Verhältnis übermittelten Daten und dem Vertrauens- bzw. Behandlungsverhältnis wird der Sache nach auch in der Gesetzesbegründung zur Einführung der elektronischen Gesundheitskarte abgestellt. Zur Begründung wird dort ausgeführt, dass die Patienten darauf vertrauen können müssen, dass die auf der Gesundheitskarte befindlichen Daten tatsächlich zur Optimierung ihrer Behandlung verwendet werden. Der Beschlagnahmeschutz gilt fort, wenn Dienstleister in Anspruch genommen werden, um die Daten zur Verbesserung von sektorübergreifenden Behandlungen unabhängig von einzelnen Behandlungseinrichtungen zu dokumentieren und für die weitere Versorgung des Patienten zur Verfügung stellen.[32]

In der hier zu begutachtenden Konstellation sollen durch behandelnde (Studien-)Ärzte im Rahmen klinischer Prüfungen ermittelte Daten an externe Dienstleister übermittelt, dort unter einem Pseudonym verwaltet und so der medizinischen Forschung zugänglich gemacht werden.[33] Durch eine 2. Stufe der Pseudonymisierung soll ggf. eine längerfristige, studienübergreifende Datenhaltung ermöglicht werden. Zwar ist vorgesehen, dass die medizinischen und patientenbezogenen Daten von einem „behandelnden (Studien-)Arzt“ erhoben werden. Offen ist jedoch, ob die Übermittlung, Speicherung und die weitere Nutzung der Daten einen (Rück)Bezug

---

Beschlagnahmeschutz im Strafverfahren. Auch ein Zeugnisverweigerungsrecht bezüglich dieser Daten steht den Forschenden - anders als insbesondere den behandelnden Ärztinnen und Ärzten - nicht zu. Zum Schutze der Forschung, vor allem aber zum Schutz der durch die Datenübermittlung und -verarbeitung Betroffenen, sollte vom Gesetzgeber deshalb sichergestellt werden, dass die bei den übermittelnden Stellen geschützten personenbezogenen medizinischen Daten auch nach ihrer Übermittlung zu Forschungszwecken den gleichen Schutz genießen. Die Datenschutzbeauftragten fordern daher den Bundesgesetzgeber auf,

* in § 203 StGB die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,

* in §§ 53, 53 a StPO für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forscher und ihre Berufshelfer zu schaffen,

* in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die Datenschutzbeauftragten sehen in diesen Vorschlägen einen ersten Schritt zu einer generellen Regelung des besonderen Schutzes personenbezogener Daten in der Forschung.“ Vgl. auch die Resolution der Delegiertenkonferenz der Arbeitsgemeinschaft der Wissenschaftlichen Medizinischen Fachgesellschaften (AWMF) am 6. Mai 1995 in Frankfurt am Main; Der Bayerische Landesbeauftragte für den Datenschutz, 16. Tätigkeitsbericht, 1994.)

[32] BT-Drs. 15/1525, S. 168.

[33] TMF-Pflichtenheft Gutachtenvergabe (Version 8), S. 13/33.

zu dem geschützten konkreten Arzt-Patienten-Verhältnis, etwa in Form einer Einbeziehung der Datenverarbeitung und -nutzung in die Behandlung des jeweiligen Patienten, aufweist. Die Formulierung in dem TMF-Pflichtenheft Gutachtenvergabe (Version 8), wonach die Daten im Rahmen klinischer Prüfungen erhoben werden und ggf. längerfristig sowie studienübergreifend gespeichert werden sollen, deutet eher auf einen ausschließlichen Forschungs- als auf einen Behandlungsbezug der Datenerhebung, -verwaltung und -übermittlung hin.

Allerdings können auch klinische Prüfungen einen Rückschluss auf eine gebotene Therapie o.ä. ermöglichen und damit auf ein spezielles Behandlungsverhältnis (rück)bezogen sein. Ein solcher Behandlungskontext soll „insbesondere bei Therapieoptimierungsstudien“ bestehen: „Hierbei werden Daten und Materialien zu Konsilzwecken („second opinion“ u.a.) verarbeitet, und die Ergebnisse wirken unmittelbar auf den betreffenden Patienten zurück.“[34] Nach unserem Eindruck scheint es sich bei diesen Studien jedoch nur um eine besondere Art von Studien zu handeln. Einen regelmäßig bestehenden Behandlungszusammenhang können wir dem TMF-Pflichtenheft Gutachtenvergabe (Version 8) hiernach nicht entnehmen.

Insoweit unterscheidet sich die vorliegende Konstellation auch von der bei der elektronischen Gesundheitskarte. Dort besteht ohne Weiteres ein Bezug der auf ihr gespeicherten Daten zu dem Behandlungs- und Beratungszusammenhang, aus dem die erhobenen Daten stammen. Zwar werden in beiden Konstellationen patientenbezogene Daten vom Arzt erhoben. Die Übermittlung und Speicherung dieser Daten erfolgt aber zu unterschiedlichen Zwecken. Während die auf der elektronischen Gesundheitskarte abgespeicherten Daten ausweislich der Gesetzesbegründung zur Optimierung der Behandlung, der Verbesserung von sektorübergreifenden Behandlungen und der weiteren Versorgung des Patienten dienen sollen[35], steht der Zweck der Patientenliste des Forschungsverbundes bislang nach den uns vorliegenden Informationen primär in einem allgemeinen medizinischen Forschungszusammenhang.

Ein entsprechender, regelmäßig vorhandener Behandlungszusammenhang wird aus der zur Begutachtung vorgelegten Konstellation daher noch nicht ersichtlich, so dass davon auszugehen ist, dass bei Gewahrsamsaufgabe durch Übermittlung oder Auslagerung patientenbezogener Daten an einen Dienstleister grundsätzlich kein Beschlagnahmeschutz mehr für diese besteht, sobald sie die Gewahrsamssphäre des Zeugnisverweigerungsberechtigten verlassen haben.

Zusammenfassend ist zu der von der Rechtsprechung und Literatur nicht bzw. nicht näher behandelten Frage somit festzuhalten, dass das Bestehen eines Beschlagnahmeschutzes nach

[34] TMF-Pflichtenheft Gutachtenvergabe (Version 8), S. 8, 3. Absatz.

[35] BT-Drs. 15/1525, S. 168.

Übertragung des Gewahrsams an den patientenbezogenen Daten auf einen IT-Dienstleister des medizinischen Forschungsverbundes maßgeblich davon abhängt, ob ein (Rück)Bezug der Datenbearbeitung und -verwendung in das konkrete schutzbedürftige Arzt-Patienten-Verhältnis besteht. Je weniger dies der Fall ist, umso weniger sind die erhobenen Daten im Gewahrsam des Dienstleisters vor Beschlagnahme geschützt. Ein solcher (Rück)Bezug ist für uns bislang jedoch nicht mit der erforderlichen Deutlichkeit erkennbar.

Bestünde ein konkreter (Rück)Bezug der an den Dienstleister weitergegebenen Daten zu dem Arzt-Patienten-Verhältnis, so könnte aus unserer Sicht auch begründet werden, dass der vorgestellte IT-Dienstleister als Dienstleister im Sinne des § 97 Abs. 2 Satz 2 StPO anzuerkennen ist und ein Beschlagnahmeschutz besteht.

Auf die Darlegung und Begründung eines entsprechenden Zusammenhangs könnte aus unserer Sicht bei der konkreten Ausgestaltung des Vertragsverhältnisses zwischen behandelndem (Studien-)Arzt und Patient geachtet werden. Dient die Datenübermittlung, -verarbeitung und -nutzung allerdings tatsächlich dem Zweck der medizinischen Forschung, kann aus unserer Sicht ein Beschlagnahmeschutz nach Gewahrsamsaufgabe des behandelnden Arztes aller Voraussicht nach nicht angenommen werden.

2.1.3 Der Dienstleister als Berufshelfer des zeugnisverweigerungsberechtigten Arztes iSd § 53a StPO

Jenseits der Fragestellung, ob der vorgestellte Dienstleister „Dienstleister“ iSd § 97 Abs. 2 Satz 2 StPO ist und er insoweit vor Beschlagnahme geschützt sein kann, stellt sich die Frage, ob der Dienstleister als Berufshelfer des Arztes iSd § 53a StPO betrachtet und als solcher gemäß § 97 Abs. 4 StPO dem Beschlagnahmeschutz unterliegen kann.

Normzweck des § 53a StPO ist es zu verhindern, dass das Zeugnisverweigerungsrecht der in § 53 StPO genannten Berufsangehörigen durch Vernehmung ihrer Hilfspersonen umgangen wird. Entsprechend ist in § 97 Abs. 4 StPO geregelt, dass auch der Beschlagnahmeschutz für den Berufshelfer des Zeugnisverweigerungsberechtigten gilt. An der Berufshelferstellung des für den Arzt tätig werdenden IT-Dienstleisters bestehen jedoch durchgreifende Zweifel.

Berufshelfer sind neben den berufsmäßig tätigen Hilfspersonen auch gelegentlich Mithelfende.[36] Im ärztlichen Bereich sind als Berufshelfer grundsätzlich anerkannt das Pflegepersonal und die mit dem Patienten befassten technischen Dienste, Labor, Röntgenabteilung, OP-Assistenten und die

[36] Der Begriff des Gehilfen iSd § 53a StPO ist insofern weiter gefasst als der der Strafnorm des § 203 Abs. 3 StGB, der nur die berufsmäßig tätigen Hilfskräfte erfasst.

Mitarbeiter des Sekretariats der Ärzte.37 Voraussetzung für eine Berufshelferstellung ist ein unmittelbarer Zusammenhang der Hilfeleistung mit der Berufstätigkeit. Die Hilfeleistung muss unterstützend sein und darf nicht lediglich äußere Bedingungen schaffen oder unterhalten. Seitens des Berufsträgers ist ein Weisungsrecht gegenüber dem Berufshelfer notwendig. Selbständige Gewerbetreibende und Externe werden angesichts dieser Voraussetzungen in aller Regel nicht als Gehilfen angesehen. So werden im ärztlichen und im Krankenhausbereich Krankenkassen, kassenärztliche Vereinigungen, privatärztliche Verrechnungsstellen und Datenbanken nicht als Berufshelfer anerkannt, da es an dem vorausgesetzten unmittelbaren Zusammenhang, auch wenn von dort bestimmte Verrichtungen für den Berufsträger ausgeführt werden.38

Insoweit ist auch der vorgestellte externe IT-Dienstleister, der im Auftrag des Arztes Patientendaten in einer Patientenliste verwaltet und nutzt sowie ggf. Erkenntnisse der Nutzung an den Arzt zum Zwecke der weiteren Behandlung oder Beratung des Patienten oder Probanden weiterleitet, nicht Berufshelfer des Arztes iSd § 53a StPO. Dieser soll als organisatorisch und rechtlich selbständige Institution weisungsunabhängig von Ärzten Daten erheben, verwalten und nutzen. Es besteht folglich kein Beschlagnahmeschutz des Dienstleisters als Berufshelfer gemäß § 97 Abs. 4 StPO.

2.1.4 Gilt auch der Dienstleister des Dienstleisters als Dienstleister iSd § 97 Abs. 2 Satz 2 StPO?

Anhaltspunkte dafür, dass auch der Dienstleister des Dienstleisters unter den Dienstleisterbegriff des § 97 Abs. 2 Satz 2 StPO subsumiert werden kann, ergeben sich weder aus dem Gesetz noch aus der Gesetzesbegründung. § 97 Abs. 2 Satz 2 StPO spricht lediglich vom Gewahrsam „eines Dienstleisters, der für die Genannten personenbezogene Daten erhebt, verarbeitet oder nutzt“ und nicht von mehreren, ggf. arbeitsteilig tätigen Dienstleistern im Rahmen einer aufgegliederten technischen Infrastruktur. Eine hiervon abweichende Ansicht scheint Hornung zu vertreten, der annimmt, dass unter den Dienstleisterbegriff nicht nur Betreiber fallen,

> „die ein komplettes Speicher- und Nutzungsmanagement anbieten, sondern auch deren Unterauftragnehmer, Anbieter, die kleine Verarbeitungen lediglich im Rahmen ihrer sonstigen Tätigkeit miterledigen, sowie die Betreiber der zugrundeliegenden technischen Infrastruktur.“[39]

[37] Senge in Karlsruher Kommentar zur StPO, 5. Aufl., § 53a, Rdnr. 2.

[38] Senge in Karlsruher Kommentar zur StPO, 5. Aufl., § 53a, Rdnr. 3.

[39] Hornung, Die digitale Identität, S. 235.

Diese Ansicht steht jedoch nicht im Einklang mit dem Gesetzeswortlaut, so dass nicht mit der erforderlichen Gewissheit davon ausgegangen werden kann, dass auch zugunsten vom Dienstleister beauftragten Dienstleistern der Beschlagnahmeschutz besteht.

Gegen die Annahme, dass ein Beschlagnahmeschutz auch bei Dienstleistern des Dienstleisters im Sinn des § 97 Abs. 2 Satz 2 StPO besteht, spricht auch die Tatsache, dass bei § 97 StPO eine dem § 53 a StPO entsprechende Regelung fehlt, die die Hilfspersonen ausdrücklich mit in den Schutzbereich der Vorschrift einbezieht. Wo das Gesetz Hilfspersonen des Zeugnisverweigerungsberechtigten in den Schutz der § 53 bzw. § 97 StPO einbeziehen möchte, geschieht dies durch ausdrückliche gesetzliche Regelung. Eine solche fehlt im Hinblick auf die Spezialvorschrift des § 97 Abs. 2 Satz 2 StPO.

Etwas anderes kann nur gelten, wenn mehrere Unternehmer als Dienstleistereinheit insgesamt durch den Zeugnisverweigerungsberechtigten mit der Bereitstellung der technischen Infrastruktur für die Erhebung, Speicherung und Nutzung im Sinne des § 97 Abs. 2 Satz 2 StPO beauftragt werden. Keinesfalls erfasst der Wortlaut des § 97 Abs. 2 Satz 2 StPO aus unserer Sicht die Beauftragung eines Unterdienstleisters o.ä. Auftragnehmern des vom Zeugnisverweigerungsberechtigten beauftragten Dienstleisters. Etwas anderes gilt jedoch, wenn der Dienstleister des Dienstleisters selbst zeugnisverweigerungsberechtigt ist (sog. abgeleiteter Gewahrsam).[40]

2.1.5 Ergebnis

Nach alledem bestehen gewichtige Gründe dafür, den Dienstleisterbegriff weit zu auszulegen und grundsätzlich auch die externe Speicherung und Nutzung patientenbezogener Daten durch Dienstleister außerhalb des Gewahrsams des zeugnisverweigerungsberechtigten Arztes im Rahmen des geschützten Arzt-Patienten-Verhältnisses dem Beschlagnahmeprivileg des § 97 Abs. 2 Satz 2 StPO zuzuordnen. Mangelt es jedoch an einem Bezug dieser Datenerhebung und -nutzung zu dem konkreten Arzt-Patienten-Verhältnis, unterfallen übermittelte, gespeicherte und genutzte Daten jedoch nicht dem Beschlagnahmeschutz des § 97 Abs. 2 StPO.

Darauf hinzuweisen ist allerdings, dass eine einschlägige Rechtsprechung und gefestigte Kommentarliteratur zu den diskutierten Fragen fehlt. Es kann nicht ausgeschlossen werden, dass Strafverfolgungsbehörden und Gerichte bei Dienstleistungsunternehmen verwahrte elektronische Patientendaten mangels Gewahrsam des Zeugnisverweigerungsberechtigten grundsätzlich als

[40] Meyer-Goßner, Kommentar zur StPO, 50. Aufl., Rdnr. 11; Schäfer in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 97, Rdnr. 31 f.

beschlagnahmefähig ansehen, soweit nicht ein Zusammenhang zur technischen Infrastruktur der elektronischen Gesundheitskarte besteht.

F2.2 Wenn ein Beschlagnahmeschutz über einen Dienstleister nicht erreicht werden kann, wäre dies über einen zugelassenen Notar als Treuhänder möglich? Welche Anforderungen stellt der von § 97 StPO geforderte (Mit-) Gewahrsam an die Verwaltung und Herausgabe von Daten? Setzt § 97 StPO voraus, das sich der Server auf dem die Patientenliste liegt in den Räumlichkeiten des Notars befindet, oder könnte der Notar ein Rechenzentrum mit der Verwahrung der Patientenliste beauftragen? Wer darf auf die Patientenliste Zugriff haben, ohne den Beschlagnahmeschutz zu gefährden?

2.2.1 Wenn ein Beschlagnahmeschutz über einen Dienstleister nicht erreicht werden kann, wäre dies über einen zugelassenen Notar als der Treuhänder möglich?

Wie unter F.2.1. festgestellt ist Beschlagnahmeschutz in vertretbarer, jedoch rechtlich nicht abgesicherter Weise, über die Aufbewahrung der Patientenliste in elektronischer Form bei einem IT-Dienstleister iSd § 97 Abs. 2 Satz 2 StPO zu erreichen, sofern ein (Rück)Bezug zum spezifischen geschützten Vertrauensverhältnis iSd § 53 StPO gegeben ist, aus dem die Daten stammen.

Zu prüfen ist ferner, ob über die Aufbewahrung der Patientenliste bei einem Notar als Treuhänder ein vergleichbarer bzw. sogar weiter gehender Schutz der Patientenliste vor einer Beschlagnahme möglich ist. Nachfolgend wird die Rechtslage für den Anwaltsnotar, nichtbeamteten Nur-Notar und dem baden-württembergischen Notar im Landesdienst, soweit dieser Aufgaben im Beurkundungsbereich und bei der sonstigen Aufgabenzuweisung auf dem Gebiet der vorsorgenden Rechtspflege wahrnimmt, dargestellt.[41]

Grundvoraussetzung der Beschlagnahmefreiheit der in § 97 Abs. 1 StPO aufgezählten Gegenstände ist nach § 97 Abs. 2 Satz 1 StPO, dass sich diese im Verfahren gegen einen Beschuldigten im Gewahrsam eines zur Verweigerung des Zeugnisses Berechtigten befinden.[42] Gem. § 18 BNotO hat der Notar die Pflicht, über die ihm bei seiner Amtsausübung bekannt gewordenen

[41] Allgemein und differenzierend zur Situation von Notaren im Landesdienst auf dem Gebiet der Freiwilligen Gerichtsbarkeit, wo § 54 iVm §§ 79ff LBG gelten, vgl. Keller, Grenzbereiche zwischen Strafrecht und Standesrecht des Notars, DNotZ 1995, 99, 100 f.

[42] Eisenberg, Beweisrecht der StPO, 5. Aufl., Rdnr. 2342.

Angelegenheiten Verschwiegenheit zu bewahren.43 Die berufsrechtliche Verschwiegenheitspflicht findet ihre notwendige Ergänzung in den Regelungen zum Zeugnisverweigerungsrecht, dort in § 53 Abs. 1 Nr. 3 StPO. Hiernach dürfen Notare über alle jene Begebenheiten das Zeugnis verweigern, die ihnen in dieser beruflichen Eigenschaft anvertraut wurden oder bekannt geworden sind, soweit sie nicht gemäß § 53 Abs. 2 StPO von der Verpflichtung zur Verschwiegenheit entbunden werden. Das Beschlagnahmeverbot des § 97 StPO knüpft im Sinne eines akzessorischen Umgehungsschutzes an das Zeugnisverweigerungsrecht des § 53 StPO an.44 Daher besteht das zur Zeugnisverweigerung berechtigende spezifische Vertrauensverhältnis auch nur gegenüber dem jeweiligen Auftraggeber, nicht jedoch gegenüber Dritten.45

Beschlagnahmefreie Gegenstände gemäß § 97 Abs. 1 Nrn. 1-3 StPO sind schriftliche Mitteilungen zwischen dem Beschuldigten und dem zeugnisverweigerungsberechtigten Notar, Aufzeichnungen, welche der Notar über die ihm vom Beschuldigten anvertrauten Mitteilungen oder über andere Umstände gemacht hat, und andere Gegenstände, auf die sich das Zeugnisverweigerungsrecht des Notars erstreckt.46 Der Kreis der durch die Begriffe „Mitteilung“, „Aufzeichnung“ und „andere Gegenstände“ bezeichneten Objekte ist damit grundsätzlich weit.

Vorliegend bestehen erhebliche Zweifel, ob es sich bei einer vom Notar als Datentreuhänder verwahrten Patientenliste überhaupt um einen Gegenstand iSd § 97 StPO handelt.

Aus der Fragestellung bei 2.6. ergibt sich der Wunsch von TMF, den Datentreuhänder für ihre Mitgliedsverbünde zu beauftragen, so dass das schützenswerte Mandatsverhältnis zwischen TMF und dem Notar zustande kommen würde. Inhalt dieses Auftragsverhältnisses wäre nach unserem Verständnis die treuhänderische Aufbewahrung und Verwaltung der Daten und Pseudonyme in der Patientenliste. In diese Patientenliste sollen Ärzte des Forschungsnetzwerkes identifizierende Daten (IDAT) des Patienten oder Probanden elektronisch übersenden können und im Gegenzug von dem treuhänderisch tätigen Notar umgehend ein Pseudonym (PID) zurückerhalten. Alle Daten, die im Verlaufe des Projekts von verschiedenen Ärzten und Forschern ermittelt werden, sollen unter Verwendung des Pseudonyms durch den Notar als Datentreuhänder verwaltet werden.47

Zweifel an der Eignung der Patientenliste als schützenswerter Gegenstand bestehen vor diesem Hintergrund insofern, als nur solche Objekte von § 97 StPO erfasst sind, die sich im Gewahrsam

---

[43] vgl. Seybold/Schippel, BNotO, 6. Aufl., § 18 Rdnr. 60 f.

[44] Meyer-Goßner, StPO, 50. Aufl., § 97 Rdnr. 1 m.w.N.

[45] Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 53 Rdnr. 7; Dahs in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 53 Rdnr. 15.

[46] Vgl. Amelung, Grenzen der Beschlagnahme notarieller Unterlagen, DNotZ 1984, 195, 196 f.

[47] TMF-Pflichtenheft Gutachtenvergabe (Version 8), S. 13/33.

des Notars befinden und die einen Zusammenhang mit Mitteilungen bzw. Gegenständen besitzen, die in dem geschützten Vertrauensverhältnis generiert worden sind. An dem Gewahrsam des Notars an der Patientenliste bestehen keine Zweifel, sofern sich

diese, wie auf einem Server gespeichert in seinen Räumen befindet und er ungehindert Zugriff auf die Patientenliste hat. Ob ein ausreichender Zusammenhang der Patientenliste und der auf ihr befindlichen Informationen mit der von § 53 StPO geschützten Berufsausübung des Notars existiert, unterliegt jedoch erheblichen Bedenken.

Das Zeugnisverweigerungsrecht sichert und schützt das persönliche Vertrauensverhältnis zwischen den Notaren und denen, die ihre Hilfe und Sachkunde in Anspruch nehmen.48 § 97 StPO verhindert so die Umgehung des Zeugnisverweigerungsrechtes und schützt damit das Vertrauensverhältnis zwischen dem Zeugnisverweigerungsberechtigten und dem Mandanten, die Vertraulichkeit in dieser Beziehung vom Mandanten gemachter Angaben, das Interesse des Notars an einer konfliktfreien Erfüllung seiner besonderen beruflichen Aufgaben und auch das Interesse der Allgemeinheit daran, dass die Dienste des Notars vorbehaltlos in Anspruch genommen werden können.49

Diese Zwecke beschreiben aber auch die Grenze der Beschlagnahmefreiheit von im Gewahrsam des Notars befindlicher Gegenstände des Mandanten. Ein Beschlagnahmeverbot ist nur dann begründet, wenn es den genannten Zwecken dient.50

Die Patientenliste stellt eine Unterlage dar, in die von einem eingeschränkten Kreis von Teilnehmern des Forschungsnetzwerkes, jedoch unabhängig vom vorgestellten Auftraggeber TMF, Daten durch Übersendung an den Notar als Treuhänder zur Aufnahme in die Patientenliste eingestellt werden können. Im Gegenzug erhalten die Ärzte und Forscher von dem Notar ein Pseudonym. Bei diesem Datenaustausch zwischen Teilnehmern des Forschungsnetzwerkes und dem Notar als Datentreuhänder handelt es sich im Verhältnis zu TMF um die Einbeziehung von Dritten, die nicht Mandanten des Notars und damit nicht von dem Schutzbereich des § 97 StPO erfasst sind. Es handelt sich ersichtlich auch nicht um Mitteilungen oder Aufzeichnungen über solche bzw. Gegenstände, die in dem geschützten Verhältnis zwischen Auftraggeber und Notar entstanden sind. Der Notar als Treuhänder erwirbt insoweit Kenntnisse von Dritten außerhalb seiner spezifischen Vertrauensbeziehung zu dem Mandanten. Diese von teilnehmenden Ärzten und

---

[48] OLG Oldenburg NJW 1982, S. 2615; LG Köln NJW 1959, 1598; Schäfer in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 97 Rdnr. 75; Senge in Karlsruher Kommentar zur StPO, 5. Aufl., § 53 Rdnr. 1.

[49] Amelung, Grenzen der Beschlagnahme notarieller Unterlagen, DNotZ 1984, 195, 198 f.

[50] Amelung, Grenzen der Beschlagnahme notarieller Unterlagen, DNotZ 1984, 195, 199.

Forschern übermittelten Kenntnisse, aus denen die Patientenliste sich zusammensetzt, sind dem Notar in der vorgestellten Konstellation der TMF als Auftraggeber des Notars nicht mehr in seiner beruflichen Eigenschaft anvertraut worden oder bekannt geworden. Das berufliche Vertrauensverhältnis ist aber das unmittelbare Schutzobjekt des notariellen Zeugnisverweigerungsrechtes gemäß § 53 Abs. 1 Nr. 3 StPO, an das der Beschlagnahmeschutz des § 97 StPO anknüpft[51], so dass ein Beschlagnahmeschutz in der vorgestellten Konstellation aus unserer Sicht abzulehnen wäre.

An diesen Bedenken würde sich auch nichts ändern, wenn nicht TMF als Auftraggeber des Notars als Datentreuhänder fungiert, sondern dieser jeweils von den teilnehmenden Ärzten oder Forschern bzw. Patienten oder Probanden mandatiert wird. Jenseits der damit einhergehenden praktischen Probleme (die Ausgestaltung der einzelnen Mandatsverhältnisse und deren Gegenstand, Vergütung des Notars etc.) müsste in dieser Konstellation hinsichtlich jedes einzelnen Mandatsverhältnisses gewährleistet sein, dass der Notar als Datentreuhänder gegenüber den im Zeitpunkt der Aufnahme in die Patientenliste noch nicht bestimmbaren Teilnehmern von seiner Verschwiegenheitspflicht gemäß § 18 BNotO befreit wird. Läge eine Entbindung von der Verschwiegenheit insoweit nicht vor, wäre der Notar gehalten, die Daten desjenigen Patienten oder Probanden getrennt aufzubewahren, was dem Sinn und Zweck der Patientenliste evident widerspricht und diese unbrauchbar machen würde. In diesem Zusammenhang dürfte es vermutlich auch ein praktisches Problem darstellen, vom Patienten bzw. Probanden eine solche Entbindungserklärung zu verlangen, wenn zugleich die Aufbewahrung bei dem Notar als Datentreuhänder dem besonderen Schutz seiner Daten vor dem Zugriff Dritter dienen soll.

Darüber hinaus ist aus unserer Sicht davon auszugehen, dass es sich bei der Aufbewahrung und Verwaltung einer Patientenliste nicht um eine iSd § 97 StPO geschützte spezifische Berufsausübung des Notars handelt. Tätigkeiten, die nicht dem Berufsbild des Berufsgeheimnisträgers entsprechen und Unterlagen, die nicht aufgrund des besonderen Vertrauensverhältnisses übergeben worden sind, sollen aber das privilegierte Zeugnisverweigerungsrecht und dementsprechend die Beschlagnahmefreiheit nicht begründen können.[52]

Schließlich spricht der Umstand, dass die Mandatierung des Notars gerade der Erreichung eines Beschlagnahmeschutzes dienen soll[53], für eine Beschlagnahmefähigkeit der Patientenliste beim Notar. In der Tat steht vorliegend nicht das durch das Mandatsverhältnis entstandene

[51] Amelung, Grenzen der Beschlagnahme notarieller Unterlagen, DNotZ 1984, 195, 199.

[52] Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 40 mw.N.

[53] vgl. TMF-Pflichtenheft Gutachtenvergabe (Version 8), S. 15/33.

Vertrauensverhältnis als Sinn und Zweck des Beschlagnahmeverbots im Vordergrund, sondern die Beschlagnahmefreiheit erscheint vielmehr als der wesentliche Zweck, der durch die Einschaltung eines Notars erreicht werden soll. Die Übergabe der Patientenliste in die notarielle Verwahrung betrifft in der hier vorgegebenen Art und Weise nicht den Gegenstand seiner typischen und speziellen beruflichen Tätigkeit. Es liegt vielmehr ein Umgehungstatbestand nahe, der durch den Schutzzweck des § 97 StPO nicht gedeckt ist.

Im Ergebnis lässt sich daher ein Beschlagnahmeschutz der Patientenliste in der uns zur Begutachtung vorgelegten Konstellation nach unserer Auffassung nicht durch die Beauftragung eines Notars als Treuhänder der Patientenliste erreichen. Dies gilt unabhängig davon, ob ein Arzt, der Forschungsverbund oder der Patient den Notar als Treuhänder mit der Aufbewahrung und Verwaltung beauftragt. Soweit sich aus 2.6. der Wunsch von TMF ergibt, den Datentreuhänder für die Mitgliedsverbünde mit der Aufbewahrung und Führung der Patientenliste zu beauftragen, ist festzustellen, dass für diese Sachverhaltskonstellation das Bestehen eines Beschlagnahmeschutzes ausgeschlossen werden kann.

Ist ein umfassender Beschlagnahmeschutz über einen Notar als Treuhänder nach der gegenwärtigen Ausgestaltung der §§ 53 f., 97 StPO, § 203 StGB mithin nicht zu erreichen, bleibt gleichwohl darauf hinzuweisen, dass die Durchsuchung und Beschlagnahme von Datenträgern bei Berufsgeheimnisträgern grundsätzlich besonders restriktiven Anforderungen im Hinblick auf die Verhältnismäßigkeit unterliegen. Das Bundesverfassungsgericht hat wiederholt betont, dass eine Durchsuchung regelmäßig die Gefahr mit sich bringt, dass unter dem Schutz des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG stehende Daten von Nichtbeschuldigten zur Kenntnis der Ermittlungsbehörden gelangen, die die Betroffenen in der Sphäre des Berufsgeheimnisträgers gerade sicher wähnen durften. Der Schutz der Vertrauensbeziehung zwischen Berufsgeheimnisträger und Mandant liege nicht allein im Interesse der individuell Betroffenen, sondern vielmehr auch im Interesse der Allgemeinheit an einer wirksamen und geordneten Rechtspflege. Diese Belange bedürfen nach Auffassung des Bundesverfassungsgerichtes einer besonderen Beachtung bei der Prüfung der Angemessenheit einer strafprozessualen Zwangsmaßnahme.54 Ferner ist darauf hinzuweisen, dass in die beim Notar beschlagnahmten Unterlagen grundsätzlich keine Einsicht für Dritte gewährt werden darf.[55]

[54] vgl. z.B. BVerfG NJW 2005, 1917, zur Beschlagnahme von Datenträgern in einem Rechtsanwalts-büro.

[55] Kanzleiter in Schippel/Bracker, BNotO, § 18, Rdnr. 62.

2.2.2 Welche Anforderungen stellt der von § 97 StPO geforderte (Mit-)Gewahrsam an die Verwaltung und Herausgabe von Daten?

Der Gegenstand muss sich im Gewahrsam des Zeugnisverweigerungsberechtigten bzw. im Gewahrsam des Dienstleisters im Sinne des § 97 Abs. 2 Satz 2 StPO befinden, damit Beschlagnahmeschutz besteht (vgl. 2.1.).56

Gewahrsam iSd § 97 StPO ist die tatsächliche Verfügungsmacht über den Gegenstand, die ein tatsächliches, von einem Herrschaftswillen getragenes Herrschaftsverhältnis, erfordert. Gewahrsam setzt nicht voraus, dass der Zeugnisverweigerungsberechtigte die Beweismittel in den Händen hält. Entscheidend ist die tatsächliche Verfügbarkeit.57 Dies gilt gleichermaßen für Gegenstände wie für Daten, die auf einem Speichermedium gesichert sind. Es ist dabei unerheblich, auf welchem Medium sich die Aufzeichnungen befinden.58.

Besonderheiten bestehen bei der Übertragung von Daten, da an dem Herrschaftsbereich des Netzbetreibers kein Gewahrsam des Dienstleisters oder des übermittelnden Arztes besteht. Dieser endet erst am Endgerät des Empfängers.59 Die Übertragung der medizinischen Daten zwischen der Proben- und Datenquelle und dem Dienstleister unterliegt daher nicht dem Beschlagnahmeschutz des § 97 StPO. Im Rahmen der Übertragung medizinischer Daten besteht gemäß § 100a StPO bei Vorliegen einer der dort aufgeführten Katalogtaten die Befugnis der Abhörung und Aufzeichnung durch die Strafverfolgungsbehörden. § 100a StPO enthält keine Privilegierung für Daten, die zwischen Leistungserbringer zu einem externen Dienstleister und umgekehrt übertragen werden.60

Hiernach ist eine wirksame Verschlüsselung der Daten sicherzustellen, damit eine Umgehung des Beschlagnahmeschutzes über die Möglichkeiten des Abhörens und Aufzeichnens von Telekommunikationsdaten verhindert bzw. deren Entschlüsselung möglichst erschwert wird.

Für das Bestehen des Beschlagnahmeschutzes ist grundsätzlich unschädlich, wenn eine andere Person an den Daten Mitgewahrsam hat, solange der Patient bzw. Proband nicht Mitgewahrsamsinhaber ist. § 97 StPO setzt keinen Alleingewahrsam des Zeugnisverweigerungsberechtigten an dem Beweismittel voraus. Ein solcher ist bereits nach dem

---

[56] Nack in Karlsruher Kommentar zur StPO, 5. Aufl., § 97, Rdnr. 8.

[57] Schäfer in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 97, Rdnr. 28.

[58] BVerfG NJW 2002, 1410.

[59] Nack in Karlruher Kommentar zur StPO, 5. Aufl., § 100a, Rdnr. 5.

[60] Hornung, Die digitale Identität, 2005, 236 m.w.N.

Wortlaut der Norm nicht erforderlich.61 Damit soll in der Praxis insbesondere der tatsächlichen Gegebenheit, beispielsweise in Anwaltssozietäten aber auch Gemeinschaftspraxen, Rechnung getragen werden. Denn regelmäßig sind nicht sämtliche dort tätigen Personen zeugnisverweigerungsberechtigt. Befinden sich die zur Beschlagnahme vorgesehenen Beweismittel im Mitgewahrsam mehrerer, sind diese daher unabhängig davon geschützt, ob sämtliche Personen zeugnisverweigerungsberechtigt sind.62 Dies gilt allerdings dann nicht, wenn der Patient bzw. Proband zugleich Mitgewahrsamsinhaber ist. Gegenstände, die (auch) der Disposition des Beschuldigten unterliegen, sind vom staatlichen Zugriff nicht ausgenommen.63

Von Bedeutung ist insoweit, dass das Datenschutzkonzept der TMF nicht vorsieht, dass der Patient oder Proband eine Art Zugangsschlüssel oder Code von der Telematikplattform oder dem Arzt erhält, um damit auf die Patientenliste bzw. seine Daten zugreifen zu können. Denn eine solche tatsächliche Zugriffsmöglichkeit zu seinen Daten könnte aus unserer Sicht durchaus einen Mitgewahrsam des Patienten an seinen Daten neben dem des Arztes gemäß § 97 Abs. 2 Satz 1 StPO und dem des Dienstleisters gemäß § 97 Abs. 2 Satz 2 StPO begründen, der zu einem Wegfall des Beschlagnahmeschutzes führt.64 Diese fehlende Zugriffsmöglichkeit des Patienten auf die Patientenliste beim Dienstleister sollte zum Schutze des Patienten bzw. Probanden aufrecht erhalten werden.

Unschädlich ist es dagegen, wenn der Patient lediglich einen rechtlichen Auskunftsanspruch hinsichtlich seiner Daten und Forschungsergebnisse hat. Der Auskunftsanspruch als solcher begründet noch keinen Mitgewahrsam.[65] Erlangt der Patient indes infolge des Auskunftsanspruchs Gewahrsam an seinen Daten, wären diese (bei ihm) wiederum beschlagnahmefähig. Patienten, die auf diesem Gewahrsam an ihren Daten (wieder-)erlangen, sollten insoweit auf den Wegfall des Beschlagnahmeschutzes hingewiesen werden. Sie könnten zugleich darauf hingewiesen werden,

---

[61] Schäfer in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 97, Rdnr. 29.

[62] Schäfer in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 97, Rdnr. 29.

[63] H.M.; vgl. BGHSt 19, 374; LG Stuttgart MDR 1990, 944; Meyer-Goßner, StPO, 50. Aufl., § 97, Rdnr. 12; Schäfer in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 97, Rdnr. 30, jeweils mit zahlreichen Nachweisen.

[64] Warda/Noelle, Telemedizin und eHealth in Deutschland: Materialien und Empfehlungen für eine nationale Telematikplattform, 2002, S. 172; vgl. Nack in Karlsruher Kommentar zur StPO, 5. Aufl., § 97, Rdnr. 8, der – allerdings nicht speziell auf Daten ausgerichtet – meint, dass nicht schon derjenige, der die Herausgabe an sich fordern kann, Mitgewahrsam hat. In der Kommentierung wird hier der rechtliche Auskunftsanspruch gemeint sein.

[65] Löffelmann in AnwaltKommentar zur StPO, § 97, Rdnr. 7; Schäfer in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 97, Rdnr. 30.

dass die ausschließliche Aufbewahrung der Gegenstände oder Daten beim Zeugnisverweigerungsberechtigten die Beschlagnahmefreiheit wieder aufleben lässt.

2.2.3 Wer darf auf die Patientenliste Zugriff haben, ohne den Beschlagnahmeschutz zu gefährden?

Wie unter b) ausgeführt, darf jedenfalls der (beschuldigte) Patient oder Proband weder Gewahrsam noch Mitgewahrsam an den Daten haben. Der Mitgewahrsam des Patienten bzw. Probanden lässt den Beschlagnahmeschutz entfallen.

Im Übrigen ist der Mitgewahrsam Dritter an der Patientenliste aus strafprozessualer Sicht unschädlich, soweit der Dienstleister iSd § 97 Abs. 2 Satz 2 StPO zumindest Mitgewahrsam hat. Dabei ist für den Beschlagnahmeschutz auch unerheblich, ob es sich bei den Dritten um zeugnisverweigerungsberechtigte Personen handelt. Der Zugriff auf die Patientenliste durch Mitarbeiter des Dienstleisters und Mitglieder des Forschungsverbundes gefährdet den Beschlagnahmeschutz daher nicht. Wir weisen jedoch darauf hin, dass Personen, die durch Zugriff Mitgewahrsam an den Patientendaten haben, als Zeugen zum Inhalt der Patientenliste befragt werden können. Sie wären auch zur Zeugenaussage verpflichtet, soweit ihnen kein eigenes Zeugnisverweigerungsrecht zusteht, was regelmäßig nicht der Fall sein dürfte. Hierdurch ist potenziell eine Umgehung des Beschlagnahmeschutzes möglich.

F2.3 Die Systematik und der Umfang des erreichbaren Beschlagnahmeschutzes sind zu beschreiben.

Der Beschlagnahmeschutz von Beweisgegenständen ist in § 97 StPO geregelt und knüpft an die Zeugnisverweigerungsrechte der §§ 52, 53 und 53a StPO an. Die Vorschrift dient der Verhinderung einer Umgehung von Zeugnisverweigerungsrechten und sichert so die geschützte Kommunikation zwischen Arzt und Patienten bzw. Probanden („Was der Mund nicht zu offenbaren braucht, darf auch der Hand nicht entrissen werden.“).

Das Beschlagnahmeverbot des § 97 StPO gilt nur für den zur Verweigerung des Zeugnisses Berechtigten.66 Dies sind u.a. Ärzte als Berufsgeheimnisträger iSd § 53 StPO sowie deren Gehilfen iSd § 53a StPO. Die Beschlagnahmeverbote gelten aufgrund der Akzessorietät zu den Zeugnisverweigerungsrechten daher nicht, wenn die zeugnisverweigerungsberechtigte Person

[66] Nack in Karlsruher Kommentar zur StPO, 5. Aufl., § 97, Rdnr. 8.

entweder nicht über ein solches verfügt oder wirksam gemäß § 53 Abs. 2 StPO bzw. § 53a Abs. 2 StPO von der Verschwiegenheitspflicht entbunden wurde.

Der Beschlagnahmeschutz ist ferner dann nicht gegeben, wenn die zeugnisverweigerungsberechtigte Person selbst Beschuldigter des Verfahrens ist.[67] So ist der Schutz des Vertrauensverhältnisses zwischen Arzt und Patient nicht darauf gerichtet, den Arzt oder Dritte vor einem Strafverfahren zu schützen.[68] Richtet sich das Strafverfahren daher nicht gegen den Patienten oder Probanden, sondern gegen den behandelnden Arzt (z.B. wegen des Vorwurfs des Abrechnungsbetruges oder eines Steuervergehens) oder einen weiteren Dritten (z.B. gegen einen Mitarbeiter des IT-Dienstleisters oder des Forschungsverbundes), besteht kein Beschlagnahmeschutz für beim Arzt oder beim IT-Dienstleister befindliche potenziell beweisrelevante Unterlagen oder Daten.

Schließlich greift § 97 StPO nicht ein, wenn die Gegenstände oder Daten durch die zeugnisverweigerungsberechtigte Person freiwillig herausgegeben und damit nicht beschlagnahmt werden. Der Verwertung steht insoweit nicht entgegen, dass sich die zeugnisverweigerungsberechtigte Person durch die freiwillige Herausgabe des Beweismittels ggfs. gemäß § 203 StGB wegen der Verletzung von Privatgeheimnissen strafbar gemacht hat.[69]

Neben dem Erfordernis des Vorliegens eines Zeugnisverweigerungsrechtes muss sich der Gegenstand im Gewahrsam des Zeugen (§ 97 Abs. 2 Satz 1 StPO), einer iSd § 97 Abs. 2 Satz 2 StPO in gleicher Weise geschützten Stelle, namentlich einer Krankenanstalt oder eines Dienstleisters, oder gemäß § 97 Abs. 4 StPO des Gehilfen iSd § 53a StPO befinden. Die Gegenstände sind grundsätzlich nur solange vor staatlichem Zugriff geschützt, wie sie sich im Gewahrsam des Zeugnisverweigerungsberechtigten befinden. Ausschließlich und gerade diese Sphäre schützt § 97 StPO.[70] Werden die vom behandelnden oder beratenden Arzt erhobenen Daten daher an außerhalb seiner Gewahrsamssphäre stehende Stellen oder Personen übertragen, die selbst nicht der ärztlichen Schweigepflicht oder einem eigenen Beschlagnahmeschutz unterliegen, entfällt dieser.

Gemäß § 97 Abs. 4 StPO erstreckt sich der Beschlagnahmeschutz auch auf Gegenstände im Gewahrsam des Gehilfen des Zeugnisverweigerungsberechtigten iSd § 53a StPO. Ausgenommen

---

[67] Nack in Karlsruher Kommentar zur StPO, 5. Aufl., § 97, Rdnr. 8; Löffelmann in AnwaltKommentar zur StPO, § 97, Rdnr. 3; BVerwG NJW 2001, 1663.

[68] Burhoff, Handbuch für das strafrechtliche Ermittlungsverfahren, 3. Aufl., Rdnr. 316 m.w.N.

[69] h.M. vgl. Löffelmann in AnwaltKommentar zur StPO, § 97, Rdnr. 4.

[70] Schäfer in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 97, Rdnr. 27.

sind aufgrund der Akzessorietät des Gehilfen zum Berufsgeheimnisträger jedoch solche Gegenstände, die beim Berufsgeheimnisträgers beschlagnahmefähig wären und solche, die sich beim tat- oder teilnahmeverdächtigen Gehilfen befinden.71

Eine Erweiterung des Beschlagnahmeschutzes erfolgt gemäß § 97 Abs. 2 Satz 2 StPO ferner in den Fällen, in denen sich die Beweismittel im Gewahrsam einer Krankenanstalt oder eines Dienstleisters befinden, der für den Zeugnisverweigerungsberechtigten personenbezogene Daten erhebt, verarbeitet oder nutzt. Vor dem Hintergrund des Schutzzwecks der Zeugnisverweigerungsrechte nach § 53 StPO und der an sie anknüpfenden Beschlagnahmeverbote bleiben die an einen Dienstleister übermittelten Daten und Unterlagen jedoch nur dann vor staatlichem Zugriff geschützt, wenn diese einen (Rück)Bezug zu dem spezifischen Arzt-Patienten-Verhältnis aufweisen, aus dem sie stammen. Hinsichtlich des Umfangs und der Systematik des Beschlagnahmeschutzes beim Dienstleister iSd § 97 Abs. 2 Satz 2 StPO nehmen wir Bezug auf die Ausführungen zu 2.1..

Der Beschlagnahmeschutz erstreckt sich gemäß § 97 Abs. 1 Nr. 1-3 StPO auf sämtliche schriftliche Mitteilungen zwischen Patient bzw. Proband und Arzt, Aufzeichnungen, die vom Arzt über den Patienten bzw. Probanden gemacht wurden sowie ärztliche Untersuchungsbefunde, auf die sich das Zeugnisverweigerungsrecht erstreckt.

In Betracht kommen als solche Gegenstände und Unterlagen insbesondere ärztliche Karteikarten72, Krankengeschichten und Krankenblätter.73 Ärztliche Untersuchungsbefunde werden im § 97 Abs. 1 Nr. 3 StPO beispielhaft als anderer nach dieser Vorschrift von der Beschlagnahme ausgenommener Gegenstand genannt. Gemeint sind damit solche Gegenstände, die sich aufgrund des zwischen dem Berufsangehörigen und einer anderen Person bestehenden Vertrauensverhältnisses im Gewahrsam des Berufsträgers befinden.74 Hierzu zählen etwa Fremdkörper, die ein Arzt aus dem Körper eines beschuldigten Patienten entfernt hat, Lichtbilder, Röntgenaufnahmen, anatomische Präparate, Kardiogramme, Elektroenzephalogramme, Blutbilder und Blutalkoholbefunde.75 Streitig ist im Hinblick auf den Beschlagnahmeschutz des § 97 Abs. 1 Nr. 3 StPO, ob es sich um Gegenstände handeln muss, die aus dem zwischen dem Zeugnisverweigerungsberechtigten und dem Beschuldigten bestehenden Vertrauensverhältnis

[71] Nack in Karlsruher Kommentar zur StPO, 5. Aufl., § 97, Rdnr. 29.

[72] LG Koblenz NJW 1983, 2100.

[73] Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 41.

[74] Schäfer in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 97, Rdnr. 75.

[75] Vgl. Schäfer in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 97, Rdnr. 77; Nack in Karlsruher Kommentar zur StPO, 5. Aufl., § 97, Rdnr. 19.

herrühren, oder ob Nr. 3 wie das Zeugnisverweigerungsrecht des § 53 StPO auch das Vertrauensverhältnis des Zeugnisverweigerungsberechtigten mit Dritten schützt. Grund für diesen Streit ist die Formulierung der Nr. 3, die von den Nr. 1 und 2 insofern abweicht, als der Beschuldigte nicht erwähnt wird. Nach überwiegender Auffassung schützt § 97 Abs. 1 Nr. 3 StPO nur ärztliche Untersuchungsbefunde, die aus dem Vertrauensverhältnis zwischen Arzt und Patient stammen.[76] Dagegen wird zwar mit beachtlichen Argumenten vertreten, dass Gegenstände, einschließlich der ärztlichen Untersuchungsbefunde, die nicht unmittelbar aus dem Vertrauensverhältnis zum Beschuldigten herrühren, der Beschlagnahme nicht zugänglich sein sollen. Diese Ansicht ist aber nicht vorherrschend. Sie argumentiert vor allem mit dem Wortlaut des § 97 Abs. 1 Nr. 3 StPO, der keine entsprechende Einschränkung vorsieht, und dem Zweck der Regelung.[77]

Zum geschützten Bereich gehören auch die Unterlagen, die schon während eines Anbahnungs- oder auch nur Beratungsverhältnisses mit dem Arzt übergeben worden sind (vgl. 2.4.).[78] Unerheblich ist die Form der Aufbewahrung und Aufzeichnung. Schriftlichen Erklärungen stehen Mitteilungen auf Ton- und Bildträgern, Datenspeichern, Abbildungen und andere vergleichbare Darstellungen gleich (§ 11 Abs. 3 StGB); gleiches gilt für elektronisch gespeicherte Mitteilungen.[79] Insofern fallen unstreitig auch bei einem Arzt oder Dienstleister gespeicherte Patientendaten in Form einer Patientenliste unter den Anwendungsbereich des § 97 StPO.

Ein bestehender Beschlagnahmeschutz an Unterlagen oder Daten ist frühestmöglich bei der Beschlagnahmeanordnung (§ 98 StPO) zu beachten. Das Vorliegen eines Beschlagnahmeverbotes macht bereits die Anordnung und Durchführung der Durchsuchung unzulässig.[80] Es hindert auch an einer einstweiligen Beschlagnahme, wenn anlässlich einer Durchsuchung Gegenstände gefunden werden, die zwar in keiner Beziehung zu dem Ausgangsverfahren der Durchsuchung stehen, aber auf die Verübung einer anderen Straftat hindeuten (§ 108 Abs. 1 StPO).[81]

Der Verstoß gegen das Beschlagnahmeverbot im Zeitpunkt der Beschlagnahme hat grundsätzlich ein Verwertungsverbot an den erlangten Gegenständen zur Folge.[82] War die Beschlagnahme

---

[76] Schäfer in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 97, Rdnr. 75 m.w.N.

[77] Vgl. Amelung, DNotZ 1984, 195, 207; Starke, Beschlagnahme von Sachverständigengutachten, in: Zur Theorie und Systematik des Strafprozeßrechts, Wolter (Hrsg.), 81, 84, LG Fulda NJW 1990, 2946.

[78] BGHSt 33, 148 = NStZ 1985, 372 m. Anm. Rogall und Hanack JR 1986, 35.

[79] BVerfG NStZ 2002, 377.

[80] Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 1.

[81] Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 108, Rdnr. 4.

[82] BGHSt 18, 227; Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 46.

zunächst rechtmäßig und treten erst später Umstände ein, die einer Beschlagnahme entgegengestanden hätten, z.B. der Wegfall eines Teilnahmeverdachts beim Zeugnisverweigerungsberechtigten, wird die Beschlagnahme nicht rückwirkend rechtswidrig. Der beschlagnahmte Gegenstand ist bzw. bleibt verwertbar.83 Entsprechendes gilt auch für den Fall, dass die Beschlagnahme zunächst rechtswidrig erfolgte, die Gründe für die Rechtswidrigkeit aber im Nachhinein wegfallen. Ergibt sich z.B. später ein Teilnahmeverdacht beim Zeugnisverweigerungsberechtigten, so ist bzw. wird die Beschlagnahme zulässig, es sei denn der Teilnahmeverdacht beruht auf dem (zunächst) rechtswidrig beschlagnahmten Gegenstand als Beweismittel.[84]

F2.4 Was ist „Untersuchung“ iSd § 53 StPO? Ist auch der forschende Arzt, Arzt iSd § 53 StPO?

Der Begriff der Untersuchung wird in § 53 Abs. 2 Satz 2 StPO verwandt und ist gleichbedeutend mit dem strafrechtlichen Verfahren. Eine ärztliche Untersuchung ist mit dem Begriff der Untersuchung in § 53 Abs. 2 Satz 2 StPO nicht gemeint.

Der forschende Arzt ist nach der herrschenden Meinung ebenfalls Arzt iSd § 53 StPO. Die strafprozessuale Kommentarliteratur stellt hinsichtlich des Arztbegriffs des § 53 StPO darauf ab, ob eine ärztliche Approbation nach § 3 BÄO vorliegt oder die Person gemäß § 2 Abs. 2 – 4 BÄO zur vorübergehenden Ausübung des Arztberufes berechtigt ist.85 Die Beschränkung des ärztlichen Berufes auf die therapeutische Tätigkeit des praktizierenden Arztes wird in Rechtsprechung und Literatur überwiegend abgelehnt.86

Es ist in Rechtsprechung und Literatur überdies anerkannt, dass auch approbierte und theoretisch arbeitende Grundlagenmediziner in Forschung und Lehre sowie der in der Verwaltung tätige Arzt den Arztberuf ausüben.87 Hierzu zählt auch der in der Industrie tätige Arzt, sofern er seine

---

[83] H.M., vgl. BGH NStZ 1983, 85; Nack in Karlsruher Kommentar zur StPO, 5. Aufl., § 97, Rdnr. 10; Schäfer in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 97, Rdnr. 147; Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 48.

[84] BGH NStZ 2001, 604; Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 48.

[85] Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 53 Rdnr. 17; Schäfer in Löwe-Rosenberg, Kommentar zur StPO, 25. Aufl., § 97 Rdnr. 33; von Schlieffen in Krekeler/Löffelmann, AnwaltKommentar StPO, § 53 Rdnr. 9; Eisenberg, Beweisrecht der StPO, 5. Aufl., Rdnr. 1270.

[86] BVerwGE 39, 100 = NJW 1972, 350; 92, 24 = NJW 1993, 3003; Hessischer Verwaltungsgerichtshof ESVGH 22, 189; Narr, Ärztliches Berufsrecht (Stand Januar 2005), A 29; Schiwy, Deutsches Arztrecht (Stand März 2006), § 2 BÄO Rdnr. 22.

[87] Hessischer Verwaltungsgerichtshof ESVGH 22, 189; BVerwGE 92, 24 = NJW 1993, 3003.

Aufgaben nur wegen seiner medizinisch-wissenschaftlichen Kenntnisse wahrnehmen kann.[88] Ausländische Ärzte können nur nach Maßgabe des § 2 Abs. 3 BÄO zeugnisverweigerungsberechtigt sein.[89]

Damit ist zunächst nur geklärt, dass auch der forschende Arzt zu dem Kreis der potenziell Zeugnisverweigerungsberechtigten des § 53 Abs. 1 Nr. 3 StPO gehört. Dies allein löst jedoch noch nicht das Zeugnisverweigerungsrecht aus, an dessen Vorliegen auch der Beschlagnahmeschutz des § 97 StPO anknüpft.

Dem Arzt steht in einem Strafverfahren gegen einen anderen ein Zeugnisverweigerungsrecht nur zu, soweit es um Informationen geht, die ihm in seiner Eigenschaft als Arzt vom Hilfesuchenden anvertraut worden oder bekannt geworden sind (§ 53 Abs. 1 Nr. 3 StPO). Maßgeblich für die Entstehung eines Zeugnisverweigerungsrechtes ist vor dem Hintergrund des Schutzzwecks des § 53 StPO (vgl. 2.1.) das individuelle Beratungs- und Behandlungsverhältnis zwischen dem Arzt und demjenigen, der seine Hilfe in Anspruch nimmt.[90] Nur und erst dieses begründet das vom § 53 StPO als schützenswert anerkannte Vertrauens- und Kommunikationsverhältnis, das den Arzt als Berufsgeheimnisträger zur Zeugnisverweigerung berechtigt.[91]

Der rein forschende Arzt, der unabhängig von einem solchen individuellen Beratungs- oder Behandlungsverhältnis zu dem Patienten oder Probanden ärztlich wirkt, wird dagegen nicht vom Schutzbereich des § 53 StPO erfasst. Er zählt daher nicht zum Kreis der zeugnisverweigerungsberechtigten Personen. Er gehört auch nicht dem möglichen Kreis der Berufshelfer des behandelnden bzw. beratenden Arztes iSd § 53a StPO an, wenn er für diesen Aufträge ausführt oder allgemein für ihn tätig ist.[92] Etwas anderes kann wiederum gelten, wenn der forschende Arzt hinzugezogen und in das Behandlungs- und Beratungsverhältnis des Arztes mit seinem Patienten eingebunden wird. Der forschende Arzt wäre dann aber nicht Berufshelfer des behandelnden bzw. beratenden Arztes iSd § 53a StPO, sondern selbst zeugnisverweigerungsberechtigt iSd § 53 Abs. 1 Nr. 3 StPO.[93]

Es ist aber auch möglich, dass der forschende Arzt zugleich oder in erster Linie als behandelnder Arzt fungiert. In diesem Fall kann ihm ein Zeugnisverweigerungsrecht i. S. v. § 53 Abs. 1 Nr. 3

---

[88] Schiwy, Deutsches Arztrecht (Stand März 2006), § 2 BÄO Rdnr. 22.

[89] Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 53, Rdnr. 17; von Schlieffen in Krekeler/Löffelmann, AnwaltKommentar StPO, § 53 Rdnr. 9.

[90] Vgl. BGH, Urteil vom 20.02.1985 – 2 StR 561/84.

[91] LG Stuttgart, Beschl. vom 17.03.1994 – 5 Ls 1248/93.

[92] Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 53a, Rdnr. 2.

[93] Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 53a, Rdnr. 2.

StPO zustehen. Diese Situation kann insbesondere bei den Investigator Initiated Trials (IIT), die sich als nicht-kommerzielle klinische Prüfungen darstellen, gegeben sein. Zwar wird der Begriff der nichtkommerziellen klinischen Prüfung im AMG nicht definiert. Es zeigt sich allerdings anhand einer Betrachtung der Begriffsdefinitionen des EU-Rechts, dass es sich dabei insbesondere um therapienah durchgeführte Studien handelt. In Erwägungsgrund Nr. 14 der Richtlinie 2001/20/EG wird etwa statuiert, dass nichtkommerzielle klinische Prüfungen, die von Wissenschaftlern ohne Beteiligung der pharmazeutischen Industrie durchgeführt werden, einen hohen Nutzen für die betroffenen Patienten haben können. Dies folgt daraus, dass bei den IITs teilweise Konzepte geprüft werden, die bereits zum anerkannten Stand des medizinischen Wissens gehören, aber dafür – noch – nicht arzneimittelrechtlich zugelassen sind. Mangels Zulassung handelt es sich dann trotz der bestehenden Behandlungssituation um eine klinische Prüfung nach AMG. Insofern besteht bei einer IIT durchaus die Möglichkeit, dass die erfassten Behandlungsdaten vollständig oder zumindest weit überwiegend reinen Behandlungszwecken dienen. Dies ist indessen nicht zwingend der Fall, da keine Kongruenz zwischen den Begriffen „nicht-kommerziell“ und „therapienah“ besteht. Dies ergibt sich schon daraus, dass auch im Rahmen von nichtkommerziellen Studien das Studiendesign unter Umständen als Kontrollgruppe eine Placebogruppe vorsehen kann und jedenfalls denjenigen Patienten, die Placebos erhalten, in keinem Fall ein therapeutischer Nutzen aus der Teilnahme an der klinischen Prüfung erwächst. Insofern bleibt es eine Betrachtung des Einzelfalls, ob eine nichtkommerzielle klinische Prüfung in erster Linie reinen Behandlungszwecken dient, ggf. trifft dies nur im Hinblick auf diejenigen Patienten zu, die tatsächlich das zu prüfende Arzneimittel erhalten. Soweit die Behandlungszwecke jedoch im Vordergrund stehen, dürfte der Forscher als behandelnder Arzt und damit als zeugnisverweigerungsberechtigt gelten.

F2.5 Wie weitgehend ist ein Beschlagnahmeschutz für die Daten einer zentralen Patientenliste erreichbar, wenn diese zumindest teilweise Daten außerhalb eines Behandlungskontextes enthält? Besteht der Beschlagnahmeschutz für die Patientenliste über die zeitliche Dauer der Behandlung? Hintergrund ist der Wunsch, dass die gewonnenen medizinischen Daten der Forschung längerfristig zur Verfügung stehen. Entsprechend langfristig und unabhängig von der Dauer der klinischen Studie sollte auch die Speicherung der identifizierenden Daten des Patienten möglich sein.

Daten außerhalb eines Beratungs- oder Behandlungskontextes sind grundsätzlich nicht von dem Beschlagnahmeschutz umfasst, auch wenn sie sich im Gewahrsam des

Zeugnisverweigerungsberechtigten, einer Krankenanstalt oder eines einschlägigen Dienstleisters im Sinne des § 97 Abs. 2 Satz 2 StPO befinden (s.o. 2.1.).

Der Beratungs- und Behandlungskontext ist allerdings sehr weit zu verstehen. Hiervon erfasst sind nicht nur die eigentliche ärztliche Behandlung oder Beratung, sondern das gesamte Vertrauens- und Kommunikationsverhältnis zwischen Arzt und Patient bzw. Probanden:

> „Die Vertrauensbeziehung erstreckt sich auf die Anbahnung des Beratungs- und Behandlungsverhältnisses. Demgemäß ist anerkannt, dass sich die Befugnis des Arztes zur Zeugnisverweigerung auch auf die Identität des Patienten und die Tatsache seiner Behandlung bezieht […].“[94]

Umfasst hiernach das Zeugnisverweigerungsrecht schon die Anbahnung des Behandlungskontextes und die Identität der Person, die den Arzt zum Zwecke der Beratung oder Behandlung aufgesucht hat, so gilt gleiches auch für solche Einzelheiten und nähere Begleitumstände ärztlicher Inanspruchnahme, die Anhaltspunkte für die Identifizierung der Person sein können.95 Insofern ist auch schon das, was die Spur zur Namhaftmachung bzw. überhaupt zum Bestehen eines Beratungs- oder Behandlungskontextes zwischen Arzt und einer konkreten Person weist, vom Zeugnisverweigerungsrecht erfasst.

Vom Zeugnisverweigerungsrecht erfasst sind ferner die eigenen Feststellungen und Beobachtungen des behandelnden Arztes.96 Irrelevant ist dabei, ob der Arzt das Wissen zufällig oder beabsichtigt erfährt.97 Es sind jegliche Kenntniserlangungen des Arztes im Rahmen des Arzt-Patienten-Verhältnisses vom Schutzbereich des § 53 StPO erfasst.

Vor dem Hintergrund dieses umfassenden Verständnisses des Behandlungskontextes und seiner Anbahnung wird deshalb zunächst genau zu prüfen sein, ob nicht doch ein Behandlungskontext der Daten in einer zentralen Patientenliste besteht.

Weisen die Daten nach Prüfung des Behandlungskontextes zumindest teilweise keinen solchen auf und existieren damit in einem Datenbestand sowohl Informationen, die einer Beschlagnahme zugänglich sind wie auch solche, die einem Beschlagnahmeverbot unterfallen, so sind die Daten nach Möglichkeit entsprechend zu trennen. Während die Informationen ohne Behandlungskontext beschlagnahmefähig sind, unterliegen die Teile mit Behandlungskontext nach wie vor nicht der Beschlagnahme. Der Beschlagnahmeschutz des § 97 StPO geht nicht dadurch verloren, dass sich

---

[94] BGH, Urteil v. 20.02.1985 – 2 StR 561/84.

[95] BGH, Urteil v. 20.02.1985 – 2 StR 561/84.

[96] Senge in Karlsruher Kommentar zur StPO, 5. Aufl., § 53, Rdnr. 18.

[97] Senge in Karlsruher Kommentar zur StPO, 5. Aufl., § 53, Rdnr. 18.

vor einem Beschlagnahmzugriff beschlagnahmefreie zusammen mit beschlagnahmefähigen Informationen in einem Datenbestand oder auf einer Unterlage befinden.

Praktisch erfolgt die Trennung der Informationen anlässlich einer Durchsuchungs- und Beschlagnahmesituation durch Sichtung der Unterlagen bzw. Daten gemäß § 110 StPO. Die Durchsicht potentiell als Beweismittel in Betracht kommender Unterlagen oder Daten ist das Mittel, um diese auf ihre Beschlagnahmefähigkeit hin zu überprüfen. Offensichtlich nach § 97 StPO beschlagnahmefreie Gegenstände sind dabei sofort und ungesichtet an den Gewahrsamsinhaber herauszugeben. Liegen die Voraussetzungen der Beschlagnahmefreiheit nicht offensichtlich vor, so erfolgt die Rückgabe der beschlagnahmefähigen Daten nach Trennung der Unterlagen oder Daten durch Sichtung, die ggfs. durch einen Richter zu erfolgen hat.98

Der Beschlagnahmeschutz besteht über die zeitliche Dauer der Behandlung hinaus, so dass im Rahmen der ärztlichen Behandlung oder Beratung erhobene Daten grundsätzlich auch nach Abschluss der Behandlung oder Beratung noch dem Beschlagnahmeschutz des § 97 StPO unterliegen. Anknüpfungspunkt für das Vorliegen des Beschlagnahmeschutzes ist nicht die Dauer der Behandlung oder Beratung, sondern das Bestehen eines Zeugnisverweigerungsrechts und der Gewahrsam an dem Beweismittel.99

Das Zeugnisverweigerungsrecht beginnt mit der Behandlungs- bzw. Beratungsanbahnung und endet durch die Entbindung von der Verschwiegenheitspflicht gemäß § 53 Abs. 2 StPO. Es dauert entsprechend § 203 Abs. 4 StGB noch nach dem Tod desjenigen fort, dessen Vertrauen zu den Berufsausübenden geschützt wird.100 Der Beschlagnahmeschutz entfällt auch nicht mit der Berufsaufgabe des Zeugen.

Der Beschlagnahmeschutz für an einen Dienstleister iSd § 97 Abs. 2 Satz 2 StPO übermittelte Informationen aus dem gemäß § 53 StPO geschützten Arzt-Patienten-Verhältnis besteht allerdings nur dann über die Dauer der Behandlung hinaus, soweit der (Rück)Bezug zum Arzt-Patienten-Verhältnis, aus dem die Daten stammen, andauert (vgl. 2.1.). Bei einem Dienstleister aufbewahrte Informationen unterliegen daher keinem Beschlagnahmeschutz mehr, wenn der (Rück)Bezug zu einem späteren Zeitpunkt wegfällt und die Informationen ausschließlich noch allgemeinen medizinischen Forschungszwecken dienen. Solange aber ein Therapiebezug zu einem späteren Zeitpunkt möglich ist und die Daten auch zu diesem Zwecke der medizinischen Forschung

---

[98] Meyer-Goßner, Kommentar zur StPO, § 110, Rdnr. 2.

[99] Nack in Karlsruher Kommentar zur StPO, 5. Aufl., § 97, Rdnr. 5; Hornung, Die digitale Identität, 2005, S. 235 m.w.N.

[100] Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 10.

weiterhin zugänglich gemacht worden sind, ist aus unserer Sicht ein den Beschlagnahmeschutz begründender (Rück)Bezug nach wie vor gegeben. Auf die Berücksichtigung eines solchen andauernden therapeutischen Bezuges über die Dauer einer Behandlung hinaus kann ggfs. im Rahmen der Vereinbarung zwischen Patient, Arzt und Dienstleister geachtet werden.

Der Beschlagnahmeschutz endet schließlich bei Gewahrsamsverlust an den Informationen, der auch unfreiwillig eintreten kann.101 Kommt ein Gegenstand daher abhanden oder wird er gestohlen, endet der Gewahrsam und der Beschlagnahmeschutz entfällt. Ein Wiedererlangen des Gewahrsams an dem Gegenstand führt zur Wiederherstellung der Beschlagnahmefreiheit.[102]

F2.6 Ist der erreichbare Beschlagnahmeschutz davon abhängig, wer einen Datentreuhänder beauftragt? Hintergrund ist der Wunsch, dass die TMF den Datentreuhänder für ihre Mitgliedsverbünde beauftragt.

Damit möglichst umfassender Beschlagnahmeschutz erreicht werden kann, ist der Datentreuhänder von dem behandelnden Arzt zu beauftragen. Gemäß § 97 Abs. 2 Satz 2 StPO gilt das Beschlagnahmeverbot nur bei dem Dienstleister, der für die Genannten, d.h. die Ärzte, Zahnärzte, Psychologischen Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten, Apotheker und Hebammen, personenbezogene Daten erhebt, verarbeitet oder nutzt. Hierzu gehört die TMF ersichtlich nicht.

Würde der Datentreuhänder durch einen Dritten, z.B. durch die TMF für ihre Mitgliedsverbünde, die mit dem Arzt kooperieren und „für ihn“ tätig sind, beauftragt werden, erscheint der Beschlagnahmeschutz aufgrund der Mittelbarkeit der Rechtsbeziehung und der Einbeziehung eines Dritten hiernach gefährdet. Denn das Bestehen einer (unmittelbaren) Auftragsbeziehung zwischen Patient bzw. Proband, behandelnden Arzt und dienstleistenden Datentreuhänder unterliegt in dieser Konstellation ersichtlich erheblichen Zweifeln. Die unmittelbare Auftragsbeziehung zwischen zeugnisverweigerungsberechtigten Arzt des Patienten und Dienstleister ist daher zu gewährleisten.

Zu unterscheiden von der Auftragsbeziehung zwischen Arzt und Dienstleister zur Verwaltung und Nutzung der patientenbezogenen Daten ist die Einrichtung der Patientenliste sowie die Schaffung der technischen und personellen Infrastruktur für die Telematikplattform. Eine Gefährdung des Beschlagnahmeschutzes ist aus unserer Sicht nicht gegeben, wenn die TMF den Datentreuhänder für die Bereitstellung der technischen Infrastruktur sowie der Schaffung der tatsächlichen und

[101] Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 13.

[102] Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 13.

rechtlichen Voraussetzungen beauftragt. Denn insoweit wird die Auftragsbeziehung zwischen Arzt und Dienstleister zur Verwaltung der patientenbezogenen Daten nicht tangiert.

F2.7 Welche besonderen rechtlichen Konsequenzen für oder Anforderungen an einen Datentreuhänder ergeben sich, wenn dieser mehrere Patientenlisten für unterschiedliche Mandanten bzw. Forschungseinrichtungen verwaltet? Hat es auf den Beschlagnahmeschutz der Daten Einfluss, ob ein zentraler Datentreuhänder oder mehrere dezentrale Datentreuhänder (z.B. eine zentrale Stelle für jede größere Stadt) existieren?

Bei der Beantwortung dieser Frage gehen wir nachfolgend vom Dienstleister iSd § 97 Abs. 2 Satz 2 StPO als Datentreuhänder aus und nehmen zu den aus strafrechtlicher Sicht gebotenen rechtlichen Vorkehrungen Stellung.

Für den Fall, dass der IT-Dienstleister mehrere Patientenlisten für unterschiedliche Forschungseinrichtungen verwaltet, hat dieser aus unserer Sicht insbesondere auf eine strikte Trennung der Patientenlisten nach den verschiedenen Auftraggebern zu achten.

Dies ist insbesondere vor dem Hintergrund einer denkbaren strafrechtlichen Relevanz geboten. Insoweit bestehen nicht gänzlich ausschließbare Risiken. Es ist gerichtlich noch nicht entschieden und in der Kommentarliteratur – soweit ersichtlich – noch nicht behandelt worden, ob Mitarbeiter eines IT-Dienstleisters aufgrund des Umstandes, dass ihnen geschützte Daten anvertraut werden, zu dem Kreis der Geheimnisträger des § 203 StGB zu zählen sind mit der Folge einer möglichen Strafbarkeit wegen der Verletzung von Privatgeheimnissen. Der Tatbestand des § 203 StGB betrifft den allgemeinen strafrechtlichen Schutz u.a. von Berufsgeheimnissen, und zwar unabhängig von Art und Form der Daten bzw. Informationsverarbeitung.

Mitarbeiter von Dienstleistern sind in § 203 Abs. 1 Nrn. 1-6 StGB nicht ausdrücklich in dem abschließenden Katalog der Geheimnisträger aufgeführt, so dass eine Strafbarkeit insoweit wohl nicht in Betracht kommt. Entsprechendes gilt wohl für die Frage, ob IT-Dienstleister aufgrund ihrer Einbindung in den spezifischen Vertrauensbereich des Berufsgeheimnisträgers iSd § 53 StPO als berufsmäßig tätige Gehilfen im Sinne des § 203 Abs. 3 Satz 2 StGB anzusehen und dem Berufsträger iSd § 203 Abs. 1 Nr. 1 StGB insofern gleichzustellen sind. Nach der gegenwärtigen Gesetzeslage und ausweislich der Kommentarliteratur ist dies abzulehnen, da externe Personen als „berufsmäßig tätige Gehilfen“ iSd § 203 Abs. 3 StGB in aller Regel als taugliche Täter

ausscheiden.103 Der sogenannte externe „Auftragsgeheimnisträger“ ist von § 203 Abs. 3 StGB nicht erfasst.

Berufsmäßig tätiger Gehilfe ist nur derjenige, der innerhalb des beruflichen Wirkungsbereichs eines Schweigepflichtigen eine auf dessen berufliche Tätigkeit bezogene unterstützende Tätigkeit ausübt. Es muss ein innerer Zusammenhang zwischen der unterstützenden Tätigkeit des Gehilfen und der berufsspezifischen Tätigkeit des Geheimnisträgers vorhanden sein. Ferner ist ein Weisungsverhältnis erforderlich. Das Verhältnis des Geheimnisträgers zum IT-Dienstleister ist in der vorgestellten Konstellation wohl nicht mit einem Verhältnis von Arbeitgeber zu Arbeitnehmer mit den daraus resultierenden Weisungsrechten des Arbeitgebers und der Weisungsunterworfenheit des Arbeitnehmers vergleichbar. Vielmehr richten sich die Rechtsbeziehungen allein nach dem Auftragsverhältnis zwischen Patient, Arzt und Dienstleister. Ein für einen berufsmäßig tätigen Gehilfen typisches und vorausgesetztes Über-/Unterordnungsverhältnis ist daher der Tendenz nach nicht vorhanden, ebenso wenig die organisatorische Einbindung des Dienstleisters in den Praxisbetrieb des Arztes.

Darüber hinaus ist der Begriff des „berufsmäßig tätigen Gehilfen“ iSd § 203 Abs. 3 StGB enger gefasst als der des „Berufshelfers“ des § 53a StPO. Zu den Berufshelfern zählen auch nur gelegentlich Mithelfende. Wie unter 2.1. näher ausgeführt, kann in der vorgestellten Konstellation der Dienstleister wohl bereits nicht als Berufshelfer iSd § 53a StPO angesehen werden. Dies lässt eine Strafbarkeit von Mitarbeitern des Dienstleisters gemäß § 203 Abs. 3 Satz 2 StGB nicht naheliegend erscheinen. Ein Meinungsstand hat sich hierzu indes noch nicht entwickelt, weshalb gesicherte Aussagen hierzu noch nicht möglich sind.

Ein strafrechtliches Risiko könnte für den gemäß § 4 f BDSG bestellten Datenschutzbeauftragten des Dienstleisters bestehen. Gemäß § 203 Abs. 2a StGB kann sich dieser wegen der Verletzung von Privatgeheimnissen strafbar machen. Gemäß § 4 f Abs. 1 BDSG haben nichtöffentliche Stellen, bei denen mehr als 9 Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, einen Datenschutzbeauftragten zu bestellen, der die Einhaltung der datenschutzrechtlichen Vorschriften kontrolliert. Ob die datenschutz- und strafrechtlichen Voraussetzungen bei den jeweiligen Dienstleistern gegeben sind, ist vom Einzelfall abhängig. Dies erscheint aber grundsätzlich möglich.

Angesichts der verbleibenden Restrisiken ist zur Vermeidung eines potenziellen Strafbarkeitsrisikos anzuraten, im Behandlungsvertrag zwischen Arzt und Patient die Einwilligung in die Weitergabe der betreffenden Daten nicht nur von dem Arzt an den Dienstleister zum bezeichneten Zweck,

[103] Tröndle/Fischer, Kommentar zum StGB, 54. Aufl., § 203, Rdnr. 21.

sondern auch die Einwilligung der Verwendung der Daten durch den Dienstleister zu medizinischen Forschungszwecken ausdrücklich aufzunehmen. Denn die Offenbarung eines Geheimnisses ist jedenfalls dann nicht tatbestandsmäßig, wenn eine wirksame Einwilligung des Geheimnisgeschützten vorliegt.104

Zum zweiten Teil der Frage ist aus unserer Sicht für einen wirksamen Beschlagnahmeschutz die möglichst unmittelbare Auftragsbeziehung zwischen behandelndem Arzt und dienstleistenden Datentreuhänder maßgeblich. Von untergeordneter Bedeutung ist, ob ein zentraler Datentreuhänder oder mehrere dezentrale Datentreuhänder im Auftrag des Arztes die personenbezogenen Daten erheben, verarbeiten oder nutzen. Auswirkungen auf den Beschlagnahmeschutz hat diese Frage nach unserer Ansicht nicht.

F2.8 Gibt es Verwendungsbeschränkungen für rechtmäßig beschlagnahmte Daten (z.B. bei der Ermittlung gegen einen Arzt)? Sind die so beschlagnahmten Daten mögliche Beweismittel gegen andere Beschuldigte/andere Straftaten wie z.B. Körperverletzung durch einen HIV-Patienten? Muss aus § 108 II StPO gefolgert werden, dass ein Verwertungsverbot nur für Strafverfahren gegen Patientinnen wegen einer Straftat nach § 218 StGB besteht?

In dem Verfahren gegen den beschuldigten Patienten ist ein rechtmäßig beschlagnahmtes Beweismittel (z.B. bei wirksamer Entbindung von der Verschwiegenheitspflicht) umfassend verwertbar.

Ist hingegen gegen das Beschlagnahmeverbot verstoßen worden, besteht ein umfassendes strafprozessuales Verwertungsverbot.105 Diese Folge gilt sowohl für das Ausgangsverfahren wie auch für ein neues oder anderes Verfahren.106 Das Verwertungsverbot kann nachträglich entfallen, wenn der Zeuge wirksam von der Verschwiegenheitspflicht entbunden wird107, aber auch durch Widerruf der Entbindungserklärung wiederhergestellt werden.108 Bis zum Widerruf erlangtes Wissen darf allerdings verwertet werden.109

---

104 Tröndle/Fischer, Kommentar zum StGB, 54. Aufl., § 203, Rdnr. 32.

105 Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 46.

106 BVerfG NJW 1972, 1123; 1977, 1489; BGHSt 18, 227, 228; Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 46; Krause/Caspary in Anwalts-Handbuch Strafrecht, Kap. E, Rz. 10 m.w.N.

107 Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 24, 48.

108 Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 25.

109 Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 47.

Richten sich die Ermittlungen gegen den behandelnden Arzt, z.B. wegen des Vorwurfs des Abrechnungsbetruges oder eines Steuervergehens, oder einen anderen Dritten, ist die Beschlagnahme von Patientendaten ungeachtet des Bestehens des privilegierten Arzt-Patienten-Verhältnisses zulässig. Das Beschlagnahmeverbot des § 97 StPO gilt nicht, wenn der Arzt selbst Beschuldigter ist.[110] Der Beschlagnahmeschutz entfällt gemäß § 97 Abs. 2 Satz 3 StPO ferner in den Fällen der sog. Verstrickung, d.h.

> „wenn die zur Verweigerung des Zeugnisses Berechtigten einer Teilnahme[111] oder einer Begünstigung, Strafvereitelung oder Hehlerei verdächtigt[112] sind oder wenn es sich um Gegenstände handelt, die durch eine Straftat hervorgebracht oder zur Begehung einer Straftat gebraucht sind oder die aus einer Straftat herrühren.“ (§ 97 Abs. 2 Satz 3 StPO)

Die in diesen Konstellationen rechtmäßig beschlagnahmten Patientendaten sind somit grundsätzlich im Strafprozess gegen den Arzt und ggf. den Mittäter oder Teilnehmer an der Tat des Arztes als Beweismittel verwertbar.[113] Es bedarf insoweit weder einer Entbindung von der Verschwiegenheitspflicht noch hindert das Sozialgeheimnis (§§ 35 SGB I, 73 SGB X) die Anwendung des § 97 Abs. 2 Satz 3 StPO.[114] Werden in einem Verfahren gegen einen Arzt oder anderen Dritten Patientendaten rechtmäßig beschlagnahmt, so kommt deren Verwertung in einem gegen den Patienten geführten Strafverfahren hingegen nicht in Betracht.

---

[110] BVerfGE 32, 373 ff.; BGHSt 38, 144 m.w.N.; Krause/Caspary in Anwalts-Handbuch Strafrecht, Kap. E, Rz. 19 m.w.N.

[111] Der Begriff der Teilnahme an der Tat des Patienten ist weit zu verstehen. Die Teilnahme durch der Arzt braucht nicht strafbar zu sein. Es genügt, wenn es sich um eine rechtswidrige Tat (vgl. § 11 Abs. 2 Nr. 5 StGB) handelt (Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 19). Entfällt der Teilnahmeverdacht gegen den Arzt im Laufe des Verfahrens gegen den beschuldigten Patienten, bleibt das Beweismittel verwertbar, sofern die Beschlagnahme zulässig war (Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 47).

[112] Besondere Verdachtsanforderungen bestehen nicht (z.B. Vorliegen eines hinreichenden oder dringenden Tatverdachts). Es reicht aus, wenn der Verdacht auf bestimmten Tatsachen beruht. In Abgrenzung dazu genügen bloße Vermutungen nicht (Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 97, Rdnr. 20).

[113] Nack in Karlsruher Kommentar zur StPO, 5. Aufl., § 97 Rdnr. 36 u.a. mit Hinweis auf BVerfG 22.05.2000, 2 BvR 291/92 und BGHSt 38, 144.

[114] Nack in Karlsruher Kommentar zur StPO, 5. Aufl., § 97 Rdnr. 36 f. m.w.N. Allerdings ist bei der Beschlagnahme und weiteren Verwertung von Patientendaten der Grundsatz der Verhältnismäßigkeit besonders zu beachten.

Die Ausgangsfrage ist daher so zu beantworten, dass rechtmäßig beschlagnahmte Beweismittel in dem jeweiligen Ausgangsverfahren Verwertung finden dürfen. Ein bei einem mitbeschuldigten Arzt oder Teilnahmeverdächtigen im Sinne des § 97 Abs. 2 Satz 3 StPO beschlagnahmter Gegenstand kann hingegen nur in dem Verfahren Verwertung finden, in dem Mittäter- oder Teilnahmeverdacht besteht oder in dem aus anderen Gründen die Beschlagnahmebeschränkungen nicht gegeben sind.115 Eine Verwertung in einem Verfahren gegen den Patienten kommt nicht in Betracht.

So dürfen z.B. rechtmäßig in einem Verfahren gegen den Arzt beschlagnahmte Patientendaten eines HIV-infizierten Patienten nicht in einem Verfahren gegen den Patienten wegen des Vorwurfs der Körperverletzung verwendet werden. Letzteres gilt aber nur, wenn das Verfahren gegen den HIV-infizierten Patienten als Beschuldigten geführt wird. Ist ein Dritter beschuldigt und führt zu seiner Entlastung an, nicht er, sondern ein bestimmter anderer HIV-Infizierter sei für die HIV-Infektion des Opfers verantwortlich, so sind die Patientendaten von letzterem in dem Verfahren gegen den ersteren beschlagnahmefähig und dürfen verwertet werden.

Für Verfahren gegen andere Beschuldigte in anderen Verfahren sind die rechtmäßig beschlagnahmten Unterlagen hiernach nicht grundsätzlich gesperrt. Sie dürfen jedoch dann nicht verwertet werden, falls in diesem anderen Verfahren z.B. wegen des Vorwurfs der Körperverletzung durch einen HIV-Patienten seinerseits die Beschlagnahmevoraussetzungen vorliegen.116

Die in der Fragestellung noch angesprochene Regelung des § 108 Abs. 2 StPO hat für die vorliegende Konstellation keine das Beschlagnahmeverbot des § 97 Abs. 2 StPO erweiternde oder beschränkende Bedeutung. § 108 Abs. 2 StPO stellt eine Sonderregelung für Zufallsfunde dar. Zufallsfunde sind bei Gelegenheit einer Durchsuchung aufgefundene Gegenstände, die zwar in keiner Beziehung zu dem Verfahren stehen, aber auf die Verübung einer anderen Straftat hindeuten (§ 108 Abs. 1 Satz 1 StPO). Solche Zufallsfunde können grundsätzlich verwertet werden, wobei auch bei Zufallsfunden das Beschlagnahmeverbot nach § 97 StPO zu beachten ist.117 Werden daher bei Gelegenheit einer rechtmäßigen Durchsuchung im Ausgangsverfahren etwa gegen den beschuldigten Patienten und/oder Arzt zufällig Gegenstände gefunden, die zwar in keiner Beziehung zu der Ausgangsuntersuchung stehen, aber auf die Verübung einer anderen Straftat hindeuten, so dürfen diese in dem anderen Verfahren nur dann in Beschlag genommen und verwertet werden, soweit für den vorgefundenen Gegenstand nicht ein Beschlagnahmeverbot gemäß § 97 StPO bestand. § 108 Abs. 2 StPO regelt den Sonderfall, dass Zufallsfunde, die

[115] H.M., vgl. Nack in Karlsruher Kommentar zur StPO, 5. Aufl., § 97, Rdnr. 9.

[116] Nack in Karlsruher Kommentar zur StPO, 5. Aufl., § 97, Rdnr. 9.

[117] Meyer-Goßner, Kommentar zur StPO, 50. Aufl., § 108, Rdnr. 1, 4, 9.

anlässlich einer Durchsuchung bei einem Arzt aufgefunden werden und den Schwangerschaftsabbruch einer Patienten betreffen, generell im Hinblick auf die Verfolgung der Patientin wegen einer Straftat nach § 218 StGB unverwertbar sind.

F2.9 Welche besonderen rechtlichen Konsequenzen für oder Anforderungen an einen Datentreuhänder ergeben sich, wenn dieser Patientenlisten für Studien verwaltet, die den Auflagen des Arzneimittelgesetzes (AMG) unterliegen?

2.9.1 Bedeutung und Stellung eines Datentreuhänders

Ein Datentreuhänder (auch als Vertrauensstelle bezeichnet) soll den Schutz der personenbezogenen Daten gewährleisten, den Eingriff in die Rechte der Betroffenen minimieren und gleichzeitig der Datenbedarf der Forschung decken[118]: Der Datentreuhänder übernimmt die Rolle eines vertrauenswürdigen Dritten. Er tritt zwischen die Daten besitzende Stelle und den Forscher oder zwischen die betroffenen Personen und den Forscher und sichert dadurch die Rechte der betroffenen Personen.

Die Institution des Datentreuhänders ist derzeit vereinzelt gesetzlich erwähnt worden, wenn auch ein allgemeiner umfassender Regelungsrahmen fehlt. So geht etwa § 12 des Hamburgischen Krankenhausgesetzes[119] (HambKHG) (Sammeln von Daten und Proben) von der Erforderlichkeit der Bestellung externer Datentreuhänder in bestimmten Fällen aus:

> „Bei einer Nutzung der Sammlung zu genetischer Forschung ist zu prüfen, ob die Sicherheit der betroffenen Personen vor einer unbefugten Zuordnung ihrer Proben und Daten es erfordert, dass die Pseudonymisierung nach den Absätzen 2 und 3 durch eine unabhängige externe Datentreuhänderin oder einen unabhängigen externen Datentreuhänder erfolgt.“

Die Vorschrift nennt jedoch weder Voraussetzungen für die Bestellung des Datentreuhänders noch die sonstigen Rahmenbedingungen für das Tätigwerden des Datentreuhänders.

Des Weiteren finden sich Regelungen über die „Vertrauensstelle“ in einigen der zur Verbesserung der Datengrundlage für die Krebsepidemiologie erlassenen **Krebsregistergesetze.** Datentreuhänder sind ansatzweise mit Vertrauensstellen in Aufgabe und Stellung vergleichbar. Die vorhandenen Regelungen zu Vertrauensstellen treffen teils präzise Aufgabenbeschreibungen.

---

[118] Vgl. Materialien zum Datenschutz unter www.datenschutz-berlin.de, Heft 28; Bizer, DuD 1999, 392, 939

[119] Gesetz v. 17.04.1991, HmbGVBl. 1991, 127, i.d. Gültigkeit zum 01.12.2007

So bestimmt etwa § 5 Hessisches Krebsregistergesetz[120]:

> **Vertrauensstelle**
>
> (1) Die Vertrauensstelle hat die gemeldeten Daten auf Schlüssigkeit und Vollständigkeit zu überprüfen und sie, soweit erforderlich, nach Rückfrage bei der oder dem Meldepflichtigen zu ergänzen oder zu berichtigen. [... -Auslassung durch den Verfasser -]
>
> (2) Die Vertrauensstelle verschlüsselt die Identitätsdaten asymmetrisch [... -Auslassung durch den Verfasser -]. Sie speichert die verschlüsselten Identitätsdaten in einer von der Registerstelle räumlich, organisatorisch und personell getrennten Datenverarbeitungsanlage. Die Speicherung dient ausschließlich dem Zweck, die Reidentifizierung der Daten für wissenschaftliche Untersuchungen nach § 9 und Auskünfte nach § 10 zu ermöglichen. [... -Auslassung durch den Verfasser -].
>
> (3) [... -Auslassung durch den Verfasser -]
>
> (4) In den nach § 9 Abs. 1 Nr. 1 genehmigten Fällen bildet die Vertrauensstelle aus den personenidentifizierenden Daten von Vergleichskollektiven Kontrollnummern und übermittelt diese an die Registerstelle zum Abgleich. Sie entschlüsselt bei Bedarf Identitätsdaten, erfragt zusätzliche Angaben von der oder dem Meldepflichtigen und veranlasst die Einwilligung der Patientin oder des Patienten nach § 9 Abs. 3.
>
> (5) Die Vertrauensstelle erteilt Auskünfte nach § 10 oder fordert dazu, soweit die Daten in der Vertrauensstelle nicht mehr vorliegen, diese von der Registerstelle an.
>
> (6) Die Vertrauensstelle veranlasst, dass alle gemeldeten Daten gelöscht und die vorhandenen Unterlagen vernichtet werden, wenn die Patientin oder der Patient der Meldung widersprochen hat, und unterrichtet die Meldepflichtige oder den Meldepflichtigen schriftlich über die Löschung.
>
> (7) Die Vertrauensstelle wirkt bei Maßnahmen länderübergreifender Abgleichung, Zusammenführung und Auswertung epidemiologischer Daten im erforderlichen Umfang mit. [... -Auslassung durch den Verfasser -]
>
> (8) [... -Auslassung durch den Verfasser -]

Vgl. auch Art. 7 des Bayerischen Krebsregistergesetzes[121]:

> (1) Die unter ärztlicher Leitung stehende Vertrauensstelle hat
>
> 1. die gemeldeten Daten nach Art. 4 Abs. 1 und 2 auf Schlüssigkeit und Vollständigkeit zu überprüfen und sie, soweit erforderlich, bei der meldenden Stelle ergänzen zu lassen,
> 2. [... -Auslassung durch den Verfasser -],
> 3. die Identitätsdaten und die epidemiologischen Daten auf getrennte Datenträger zu übernehmen,

[120] G. v. 17.10.2001 (GVBl. I 2001, 582) i. d. Gültigkeit v. 01.12.2007

[121] G. v. 25.07.2000, GVBl S. 274, zuletzt geändert durch G. vom 24.12.2005, GVBl. S. 652

4. die Identitätsdaten nach Art. 10 Abs. 1 zu verschlüsseln und Kontrollnummern nach Art. 10 Abs. 2 zu bilden,
5. [... -Auslassung durch den Verfasser -]
6. in den nach Art. 11 Abs. 1 genehmigten Fällen personenidentifizierende Daten abzugleichen oder Identitätsdaten zu entschlüsseln, nach Maßgabe des Art. 11 Abs. 3 Satz 2 zusätzliche Angaben von dem Meldenden zu erfragen, die Erteilung der Einwilligung des Patienten, soweit erforderlich, zu veranlassen, die Daten an den Antragsteller zu übermitteln sowie die nach Art. 11 Abs. 1 und 3 Satz 2 erhaltenen und die nach Art. 11 Abs. 1 erstellten Daten zu löschen,
7. in Fällen des Art. 12 Abs. 1 die Auskunft zu erteilen oder, soweit die Daten in der Vertrauensstelle nicht mehr vorhanden sind, von der Registerstelle die erforderlichen Daten anzufordern,
8. wenn der Patient der Meldung widersprochen hat, zu veranlassen, dass die gemeldeten Daten gelöscht und die vorhandenen Unterlagen vernichtet werden; sie haben die Löschungen zu zählen und den Arzt oder Zahnarzt über die erfolgte Löschung schriftlich zu unterrichten,
9. [... -Auslassung durch den Verfasser -],
10. [... -Auslassung durch den Verfasser -].

(2) Die Vertrauensstelle hat die nach Art. 7 des Bayerischen Datenschutzgesetzes erforderlichen technischen und organisatorischen Maßnahmen zu treffen. Sie hat insbesondere zu gewährleisten, dass die zeitweise vorhandenen, personenidentifizierenden Daten nicht unbefugt eingesehen oder genutzt werden können.

Den Einsatz von Datentreuhändern wird auch in der Stellungnahme des Bundestages zur Technikfolgenabschätzung hinsichtlich Biobanken angesprochen:[122] :

> Mit dem Instrument der Treuhandschaft wird eine intermediäre Instanz angesprochen, welche die personenbezogene Zuordnung von Proben zu (Gen-)Daten und weiteren Datensätzen kontrolliert. Darüber hinaus könnten Treuhänder weitere Aufgaben übernehmen, z. B. um Transparenz- und Rechenschaftspflichten zu genügen, aber auch einen öffentlichen Diskurs zu befördern, indem Spender/Probanden und Öffentlichkeit zu Forschungs- und Nutzungsprioritäten konsultiert sowie regelmäßige Berichte über kommerzielle Nutzung oder Resultate aus den Forschungen mit Proben und Daten aus Biobanken vorgelegt werden. Unterschiedliche Vorstellungen gibt es über mögliche Modelle und Trägerschaften. Treuhänder können für die Organisation von Biobanken als unabhängige intermediäre Instanz eingesetzt werden. Sie können sowohl als gemeinnützige, privatwirtschaftliche oder staatliche Institution und in bestimmten Formen der Kooperation auftreten, die ihrerseits wieder Beauftragte verschiedener Interessengruppen umfasst. Welcher Organisationsform der Vorrang zu geben ist, hängt vom Einzelfall ab.

[122] Bundestags-Drucks. 16/5374 (betr. Technikfolgenabschätzung bei Biobanken), S. 84

Weiter heißt es auf S. 103 dieser Stellungnahme:

> Datentreuhänder
> Der Datentreuhänder tritt zwischen die datenbesitzende Stelle und den Forscher und sichert dadurch die Rechte des Betroffenen. Er anonymisiert oder pseudonymisiert die von der datenbesitzenden Stelle übermittelten personenbezogenen Daten und übermittelt nur die anonymisierten bzw. pseudonymisierten Daten an den Forscher weiter. Auf diese Weise bleibt der Kreis derjenigen Stellen, die Kenntnis von personenbezogenen Daten erhalten, eng begrenzt, und die Datensicherheit kann effektiv gewährleistet werden. Die damit durch den Datentreuhänder wahrgenommene Funktion eines „vertrauenswürdigen Dritten“ kann noch verstärkt werden, wenn dieser einer Berufsgruppe angehört, die gesetzlich zur Verschwiegenheit verpflichtet ist und deren Unterlagen und Daten einem Beschlagnahmeschutz unterliegen (Beispiele: Rechtsanwälte, Notare). Datentreuhänder werden bereits von einigen medizinischen Kompetenznetzen eingesetzt.

Ingesamt lässt sich der Datentreuhänder als eine vielfach für medizinische Datensammlungen vorgeschlagene und anerkannte Institution ansehen, die jedoch bislang noch nicht im ausreichenden Maße vom Gesetzgeber reguliert wurde. Der aufgezeigte Rechtsrahmen für Vertrauensstellen sowie die Äußerungen des Bundestages in seiner Stellungnahme geben jedoch eine Orientierungshilfe, auf die an vielen Stellen dieses Gutachtens zurückgegriffen werden wird.

2.9.2 Der Datentreuhänder im Pflichtengefüge von klinischen Prüfungen nach dem AMG

2.9.2.1 Grundlegende Anforderungen für die Einbindung

Wird ein Datentreuhänder für klinische Prüfungen herangezogen – hier soll zunächst die Verwaltung von Patientenlisten durch den Datentreuhänder im Rahmen solcher klinischer Prüfungen untersucht werden –, so können die rechtlichen Möglichkeiten einer Einbindung unterschiedlich sein. Es ist insbesondere zu klären, ob es sich um eine Art Delegation der Erfüllung von gesetzlichen Pflichten handelt oder der Datentreuhänder als völlig unabhängiger Dritter hinzutritt. Jeweils isoliert betrachtet, würde keine der beiden Alternativen eine für alle Beteiligten zufriedenstellende Lösung bieten. Die Stellung des Datentreuhänders als eine vertrauenswürdige und neutrale Person würde es einerseits nicht zulassen, den Datentreuhänder gänzlich als eine Art Erfüllungs- oder Verrichtungsgehilfen des Sponsors oder der Prüfärzte anzusehen (eine Delegation einzelner Aufgaben im Rahmen klinischer Prüfungen auf den Datentreuhänder ist aber erlaubt). Insbesondere darf der Datentreuhänder nicht weisungsgebunden sein. Andererseits wäre es im Rahmen klinischer Prüfungen auch unbefriedigend oder unzureichend, wenn der Datentreuhänder derart unabhängig wäre, dass für die beteiligten Prüfärzte und Sponsoren nicht mehr gewährleistet wäre, dass sie ihren eigenen gesetzlichen Rechten und Pflichten nachkommen können. Es bietet

sich daher an, eine Lösung in der Mitte zu suchen und demnach eine **vertragliche Vereinbarung** mit dem Datentreuhänder anzustreben, die

- die Stellung des Datentreuhänders als neutrale und die Vertraulichkeit wahrende Stelle voraussetzt, gleichzeitig aber
- sicherstellt, dass alle an der klinischen Prüfung Beteiligten (Sponsoren, Monitore, Prüfärzte, Behörden, Studienteilnehmer etc.) ihren gesetzlich normierten Rechten und Pflichten nachkommen können.

Die Vereinbarung müsste deswegen in Vertragsform erfolgen, da derzeit keine gesetzlichen Rahmenbedingungen für einen Datentreuhänder existieren und demnach die Situation der an der klinischen Prüfung Beteiligten unsicher wäre. Insbesondere ist der Datentreuhänder derzeit nicht im Arzneimittelrecht als **Normadressat** benannt. Das AMG formuliert für klinische Studien die Verantwortlichkeit vielmehr wie folgt:

> § 40 Allgemeine Voraussetzungen der klinischen Prüfung
> (1) Der Sponsor, der Prüfer und alle weiteren an der klinischen Prüfung beteiligten Personen haben bei der Durchführung der klinischen Prüfung eines Arzneimittels bei Menschen die Anforderungen der guten klinischen Praxis nach Maßgabe des Artikels 1 Abs. 3 der Richtlinie 2001/20/EG einzuhalten.

(Neben die gesetzlichen und untergesetzlichen Vorgaben können im Einzelfall auch Auflagen der Ethikkommission treten.)

Daher können den Datentreuhänder ohne entsprechende Vereinbarungen über seine Einbindung in die spezifischen Rechtspflichten des Arzneimittelrechts keine rechtlichen Verpflichtungen treffen.

Gleiches muss im Hinblick auf die Vorschriften der GCP-V gelten. Auch die in der GCP-V enthaltenen gesetzlichen Verpflichtungen können den Datentreuhänder nicht direkt treffen. Der Datentreuhänder wird auch innerhalb der GCP-V nicht erwähnt; er wird nicht als Beteiligter oder gar Verantwortlicher einer klinischen Prüfung benannt. Allerdings liegt in der Einrichtung eines Systems, das einen Datentreuhänder vorsieht, nicht automatisch ein Konflikt mit den Vorgaben der GCP-V. Denn die GCP-Grundsätze können insoweit nicht als ein abschließendes organisatorisches Gerüst für klinische Prüfungen angesehen werden. Entscheidend ist hier ausschließlich, dass die Vorgaben der GCP-V insgesamt eingehalten werden. Sofern also eine organisatorische Einbindung des Datentreuhänders im Rahmen einer klinischen Prüfung erfolgen soll, ist daher zwingend erforderlich, dass die Figur des Datentreuhänders mit den GCP-Prinzipien in Einklang steht. Der Datentreuhänder muss in das Organisationssystem der klinischen Prüfung derart eingebunden werden, dass die Beteiligten ihre gesetzlichen Pflichten ordnungsgemäß erfüllen können. So hat bspw. der Sponsor gemäß § 6 GCP-V bei verblindeten Prüfpräparaten ein System zur unverzüglichen Entblindung zu etablieren, das eine sofortige Identifizierung und, sofern

erforderlich, eine unverzügliche Rücknahme der Prüfpräparate ermöglicht. Dabei ist sicherzustellen, dass die Identität eines verblindeten Prüfpräparates nur so weit offen gelegt wird, wie dies erforderlich ist. Im Falle der Einbindung eines Datentreuhänders kommt diesem im Rahmen der Entblindung die Bedeutung einer zusätzlichen, gleichsam zwischengeschalteten Instanz zu. Demnach muss der Sponsor an dieser Stelle dafür Sorge tragen, dass das Verfahren zur unverzüglichen Entblindung auch unter Mitwirkung des Datentreuhänders entsprechend den gesetzlichen Voraussetzungen des § 6 GCP-V erfolgen kann. Es ist insgesamt erforderlich, dass die nach der GCP-V Verantwortlichen auch unter Einbeziehung des Datentreuhänders in der Lage sind, ihre gesetzlichen Aufgaben ordnungsgemäß wahrzunehmen. Dabei verbleibt im Übrigen die gesetzliche („Letzt“-)Verantwortung stets bei den von der GCP-V benannten verantwortlichen Personen, insbesondere Sponsor und Prüfarzt.

2.9.2.2 Zulässigkeit der Einbindung des Datentreuhänders

Die für klinische Prüfungen bestehenden gesetzlichen Regelungen stehen einer vertraglichen Einbindung eines Datentreuhänders für die Verwaltung von Patientenlisten nicht entgegen, wenn gewährleistet werden kann, dass das im Arzneimittelrecht definierte Verantwortlichkeitsgefüge sowie der Datenschutz eingehalten werden. Die Einbindung eines Datentreuhänders darf, anders ausgedrückt, zum einen nicht dazu führen, dass der Sponsor oder der Prüfarzt jeweils ihre Rechte und Pflichten aus dem AMG und GCP-V nicht mehr einhalten bzw. einhalten können (dazu sogleich 2.9.3). Zum anderen muss zur Wahrung des Datenschutzes eine ausdrückliche Patientenweinwilligung hinsichtlich der Einbindung eines Datentreuhänders bestehen (dazu unten 2.9.4 b).

2.9.3 Verantwortung für die Patientendaten bei klinischen Prüfungen

Im Folgenden sind die grundlegenden Anforderungen an die Verwaltung von Patientendaten bei klinischen Prüfungen zu beschreiben. Diese Gefüge von Rechten und Pflichten bildet den Rahmen, den der Datentreuhänder bei seinen Diensten zu beachten hat. Vertragliche Vereinbarungen sollten darauf abzielen, den Datentreuhänder zur Einhaltung des nachgehend aufgeführten gesetzlichen Rahmens zu verpflichten bzw. ihn in diesen Rahmen soweit möglich und nötig, zu integrieren. Allerdings ist dabei zu betonen, dass ein entsprechender Vertrag mit dem Datentreuhänder die gesetzliche Verantwortung der übrigen Beteiligten nicht verschieben kann. Insbesondere verbleibt die „Letztverantwortung“ bei den gesetzlich verpflichteten Personen.

2.9.4 Datenschutzrechtliche Einwilligung der Patienten

a) Allgemeine datenschutzrechtliche Einwilligung

Die datenschutzrechtliche Einwilligung ist eine notwendige Voraussetzung für die Durchführung einer klinischen Studie und erfolgt zusätzlich zu der Einwilligung in die Studienteilnahme. § 40 Abs. 2a AMG normiert die besonderen Voraussetzungen für die informierte datenschutzrechtliche Einwilligung der betroffenen Person (§ 3 Abs. 2a GCP-V). Danach ist die betroffene Person über Zweck und Umfang der Erhebung und Verwendung personenbezogener Daten, insbesondere von Gesundheitsdaten zu informieren. Sie ist insbesondere auch darüber zu informieren, dass die erhobenen Daten soweit erforderlich

- zur Einsichtnahme durch die Überwachungsbehörde oder Beauftragte des Sponsors zur Überprüfung der ordnungsgemäßen Durchführung der klinischen Prüfung bereitgehalten werden,
- pseudonymisiert an den Sponsor oder eine von diesem beauftragte Stelle zum Zwecke der wissenschaftlichen Auswertung weitergegeben werden,
- im Falle eines Antrags auf Zulassung pseudonymisiert an den Antragsteller und die für die Zulassung zuständige Behörde weitergegeben werden,
- im Falle unerwünschter Ereignisse des zu prüfenden Arzneimittels pseudonymisiert an den Sponsor und die zuständige Bundesoberbehörde sowie von dieser an die Europäische Datenbank weitergegeben werden.

Zur informierten datenschutzrechtlichen Einwilligung gehört auch die Aufklärung darüber, dass die Einwilligung nach Absatz 1 Satz 3 Nr. 3 c AMG unwiderruflich ist. Im Falle eines Widerrufs der nach Absatz 1 Satz 3 Nr. 3 Buchstabe b erklärten Einwilligung die gespeicherten Daten weiterhin verwendet werden dürfen, soweit dies erforderlich ist, um die Wirkungen des zu prüfenden Arzneimittels festzustellen, sicherzustellen, dass schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden oder um der Pflicht zur Vorlage vollständiger Zulassungsunterlagen zu genügen (§ 40 Abs. 2a S. 2 Nr. 3 AMG). Die betroffene Person muss zudem darin einwilligen, dass die Daten bei den genannten Stellen für die auf Grund des § 42 Abs. 3 AMG bestimmten Fristen gespeichert werden (§ 40 Abs. 2a S. 2 Nr. 4 AMG).

Gemäß § 40 Abs. 2a S. 3 AMG haben im Falle eines Widerrufs der nach § 40 Abs.1 S. 3 Nr. 3b AMG erklärten Einwilligung die verantwortlichen Stellen unverzüglich zu prüfen, inwieweit die gespeicherten Daten für die in § 40 Abs. 2a S. 2 Nr. 3 AMG genannten Zwecke noch erforderlich sein können. Nicht mehr benötigte Daten sind gemäß § 40 Abs. 2a S. 4 AMG unverzüglich zu löschen. Im Übrigen sind die erhobenen personenbezogenen Daten nach Ablauf der auf Grund des § 42 Abs. 3 AMG bestimmten Fristen gemäß § 40 Abs. 2a S. 5 AMG zu löschen, soweit nicht gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen. Dies bedeutet grundsätzlich für die klinische Praxis, dass jeder Beteiligte an der klinischen Prüfung zu den jeweiligen Einsatzzeiten – d.h. zu den jeweiligen Zeitpunkten des Ablaufs der Schutzfristen –

alle erhobenen Daten auf ihre weitere Aufbewahrungsmöglichkeit hin überprüfen muss. Zwar mögen die dargestellten Anforderungen praktisch nur schwer erfüllbar sein; gleichwohl handelt es sich bei diesen Vorgaben des AMG um zwingende öffentlichrechtliche Vorschriften, nicht etwa um vertraglich dispositives Recht. Insofern müssen die an der klinischen Prüfung Beteiligten sich diesen gesetzlichen Vorgaben auch unterwerfen.

b) Patienteneinwilligung über die Einbindung des Datentreuhänders in die klinische Prüfung

Die Einbindung des Datentreuhänders in die klinische Prüfung gem. § 40 AMG setzt zunächst voraus, dass er in legitimer Weise über die Daten der von der klinischen Studie betroffenen Personen (§ 3 Abs. 2a GCP-V) verfügen darf. Diese Legitimation kann nach derzeitigem Recht wohl nur über eine **ausdrückliche Einwilligung der betroffenen Personen** geschehen[123]. Eine Nutzung ohne ausdrückliche Einwilligung wäre nämlich allenfalls möglich, wenn sie ohne einen Personenbezug (anonymisiert) oder auf Grundlage des Forschungsprivilegs nach § 28 Abs. 6 Nr. 4 BDSG erfolgen würde. Eine anonymisierte Nutzung liegt beim Datentreuhänder aber gerade nicht vor, da er die Verknüpfung zwischen den Daten der klinischen Studie und der jeweils betroffenen Person herstellen kann und ggf. soll. Auch dürften das **Forschungsprivileg** nach § 28 Abs. 6 Nr. 4 BDSG **nicht** anwendbar sein. Die Vorschrift erfordert, dass die begehrte Erhebung, Verarbeitung bzw. Nutzung von personenbezogenen Daten nach § 3 Abs. 9 BDSG (hier: gesundheitsbezogene Daten) zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Zunächst ist die Regelung des § 28 Abs. 6 Nr. 4 BDSG für den Bereich der klinischen Forschung nur äußerst begrenzt anwendbar. Aufgrund der Kollisionsnorm § 1 Abs. 3 BDSG gehen spezialgesetzliche Regelungen für personenbezogene Daten auf Bundesebene, einschließlich Regelungen berufsrechtlicher Art, dem BDSG vor. In § 40 AMG sowie den Regelungen der GCP-V finden sich gerade spezielle Regelungen für den Umgang mit Daten der von der klinischen Studie betroffenen Person. Diese Regelungen treffen bereits eine Grundwertung dahingehend, dass die Patientendaten grundsätzlich nur dem Prüfarzt zugänglich sein sollen und eine Übermittlung an den Sponsor (und ggf. an Behörden und die Ethikkommission) in pseudonymisierter Form zu erfolgen hat. Hinzu kommt die ärztliche Schweigepflicht, die ebenfalls der Regelung in § 28 Abs. 6 Nr. 4 BDSG vorgeht[124]. Der Datentreuhänder ist zudem ein **Dritter**, da er – anders als in den

[123] die andere Möglichkeit wäre, dass gesetzliche Befugnisnormen existieren, vgl. auch Bizer, DuD 1999, 392, 394; Materialien zum Datenschutz unter www.berlin-datenschutz.de, Heft 28.

[124] Simitis, Kommentar zum BDSG, 6. Aufl., § 28, Rn. 14

Fällen der Auftragsdatenverarbeitung i. S. v. § 11 BDSG - nicht weisungsgebunden ist. Es findet daher eine „Übermittlung“ im Sinne des BDSG an den Datentreuhänder als Dritten statt.

Wenn somit eine ausdrückliche Einwilligung erforderlich ist, so ist zu klären, bei welchem **Anlass** und welcher **Form** diese Patienteneinwilligung in die Einbindung eines Datentreuhänders erfolgen kann. Es empfiehlt sich, die Einwilligung anlässlich der datenschutzrechtlichen Einwilligung in die Studie gem. § 40 Abs. 2a S. 1 und S. 2 AMG durchzuführen. Die Informierung über die Einbindung eines Datentreuhänders fügt sich thematisch in den Anlass der Informierung nach § 40 Abs. 2a ein, da diese gem. S. 1 „Zweck und Umfang der Erhebung und Verwendung personenbezogener Daten, insbesondere Gesundheitsdaten“ umfasst und in dem Katalog (Nr. 1 bis Nr. 4) gem. S. 2 nur ein Mindeststandard vorgegeben wird (vgl. Wortlaut: „*insbesondere* darüber zu informieren …“).

Allerdings ist zu beachten, dass der Datentreuhänder ggf. nicht nur die Studie überwacht, sondern auch mit Blick auf die spätere Erstellung einer medizinischen Sammlung (Forschungs- oder Kompetenznetz) eingebunden wird. Auf eine solche Zweckänderung sind die Patienten ggf. ausdrücklich hinzuweisen. Bei der datenschutzrechtlichen Einwilligungserklärung der Studienteilnehmer gem. § 40 Abs. 2a AMG kann somit **zusätzlich, also separat,** die (informierte) Einwilligungserklärung über die **treuhänderische Identitätsverwaltung** patientenbezogener Daten durch den **Datentreuhände**r eingeholt werden. Diese spezifische Einwilligungserklärung über die Einbindung des Datentreuhänders müsste den allgemeinen Anforderungen an eine **datenschutzrechtliche Einwilligung** genügen. So gilt hinsichtlich des Inhalts § 4, und hinsichtlich der Form § 4a BDSG. Die betroffene Person müsste also über die die **Identität des Datentreuhänders, die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung** und die Kategorien von Empfängern informiert werden. Die Informierung sollte auch ggf. den Umstand erfassen, dass und in welchem Umfang und mit welchem Zweck die Daten des Patienten in einem **Kompetenznetz gespeichert** werden, auf den auch andere Forscher oder Ärzte – unter Pseudonymisierung des betroffenen Patienten – Zugriff haben. Sehr wichtig ist, dass dem Betroffenen klar werden sollte, dass es nicht allein um den Behandlungskontext geht, sondern (auch) das Forschungsinteresse Grund für die Verwendung der Daten sein wird.

Die Einwilligung ist zudem nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Die Einwilligung bedarf zudem der **Schriftform**. Da die Einwilligung über die Einbindung des Datentreuhänders zusammen mit der „normalen“ datenschutzrechtlichen Einwilligung in klinische Studien gem. § 40 Abs. 2a AMG zusammen durchgeführt werden würde, dürfte es ratsam sein, die Erklärung eigens hervorzuheben bzw. abzusetzen und die Patienten auf sie eigens hinzuweisen. Wenn eine datenschutzrechtliche Einwilligung zusammen mit anderen Erklärungen

schriftlich erteilt wird, ist sie gem. § 4a Abs. 1 S. 4 BDSG besonders hervorzuheben. Zudem gebietet der Rechtsgedanke von § 305c Abs. 1 BGB, Klauseln mit Überraschungscharakter nicht ohne besondere Hervorhebung oder besonderen Hinweis zu benutzen. Die Einbindung von Datentreuhändern dürfte in diesem Sinne eine bislang noch ungewohnte Bestimmung für die Patienten sein, so dass sie darauf extra hingewiesen werden sollten.

2.9.5 Pseudonymisierungspflicht und Reidentifikation

Aus dem AMG und der GCP-V ergibt sich, dass vor der Übermittlung und/oder der Dokumentation von personenbezogenen Daten durch den Prüfer (§ 4 Abs. 25 AMG) oder den Sponsor (§ 4 Abs. 24 AMG) diese unter Verwendung von Identifizierungscodes zu **pseudonymisieren** sind, vgl. etwa § 40 Abs. 2a S. 2 Nr. 1 b bis d AMG und §§ 12, 13 GCP-V. Ausnahmsweise ist es bestimmten Personen zu bestimmten Zwecken gestattet, die personenbezogenen Daten in nicht anonymisierter und nicht pseudonymisierter Weise zu erhalten, z.B. beim Monitoring klinischer Studien. Eine solche Situation hat § 40 Abs. 2a Nr. 1 a AMG vor Augen. Die Vorschrift normiert, dass die betroffen Person darüber zu informieren ist, dass die Daten – soweit erforderlich – zur Einsichtnahme durch die Überwachungsbehörde oder Beauftragte des Sponsors zur Überprüfung einer ordnungsgemäßen Durchführung der klinischen Prüfung bereitgehalten werden. Genauer gesagt, sind es in diesen Fällen etwa das BfArM[125] und das Monitoring-Personal des Sponsors (oder einer Clinical Research Organisation, „CRO“), welche direkten Zugang zu solchen „source data“ hätten.[126]

Die Pseudonymisierungspflicht entspricht auch der Verpflichtung aus § 3a BDSG zur Datenvermeidung und -sparsamkeit sowie einer möglichst pseudonymisierten Verarbeitung. Das BDSG sowie das sonstige allgemeine Datenschutzrecht wird durch die Spezialregelungen von AMG und GCP-V nicht völlig verdrängt, sondern bleibt subsidiär (vgl. auch Kollisionsnorm § 1 Abs. 3 BSDG) anwendbar.[127]

Die Pseudonymisierung hat bei klinischen Prüfungen zur Folge, dass in der Regel nur die behandelnden Ärzte die Zuordnung der Studiendaten zu einer bestimmten betroffenen Person

[125] *Bundesamt für Arzneimittel und Medizinprodukte* als zuständige Bundesoberbehörde nach § 77 AMG. Bei klinischen Studien in den USA bspw., wäre die Aufsichtsbehörde FDA

[126] Weisser/Bauer, MedR 2005, 339, 342.

[127] Weisser/Bauer, MedR 2005, 339, 341; Kloesel/Cyran, Kommentar zum AMG, § 40 Rn. 53 (Stand: 101. Akt.-Lief. 2006).

kennen. Die empfangende Stelle darf nach Übermittlung der Daten nur über den behandelnden Arzt **Kontakt zu dem Betroffenen** aufnehmen.[128]

Ohne Datentreuhänder oder sonstige dritte Dienstleister erfolgt also die Verwaltung der Daten der Studienteilnehmer durch die Prüfärzte bzw. in pseudonymisierter Form – durch den Sponsor. Die Einbindung des Datentreuhänders muss erfolgen, ohne den beschrieben, vom AMG und der GCP-V vorgesehenen, **Datenfluss klinischer Prüfungen** in Frage zu stellen. Zudem dürfen die Bestimmungen über die datenschutzrechtliche Einwilligung der betroffenen Personen in § 40 Abs. 2a S. 2 (Nr. 1 bis Nr. 4) AMG durch die Einbindung des Datentreuhänders nicht in Frage gestellt werden, denn mit dieser informierten Einwilligung hat der Patient gerade gewissen Arten einer Datennutzung zugestimmt. Die Bestimmungen des § 40 Abs. 2a S. 1 Nr. 2 AMG, wonach die betroffene Person darüber informiert wird, dass die Daten pseudonymisiert an den Sponsor (Nr. 2b) und ggf. an die für die Zulassung zuständige Behörde (Nr. 2c) und die Bundesoberbehörde (Nr. 2d) **weitergegeben** werden, verlieren jedenfalls ihre Gültigkeit nicht allein deshalb, weil ein Datentreuhänder eingeschaltet wird. Denn auch in diesem Fall erhält der Sponsor bzw. die Behörde nur pseudonymisierte Daten. Lediglich ändert sich, dass die Verwaltung des Pseudonyms bzw. die Identitätsverwaltung nicht etwa durch den Prüfarzt bzw. die Prüfeinrichtung, sondern durch einen Datentreuhänder erfolgt.

Auch muss im Sinne von § 40 Abs. 2a Nr. 1a AMG die Überwachung durch Behörden und durch das Monitoring-Personal möglich bleiben. Es kann sich für die Sponsor empfehlen, mittels **vertraglicher Vereinbarungen** die notwendige Kooperation seines Monitoring-Personals mit dem Datentreuhänder sicherzustellen. Es kann sich zusätzlich empfehlen, der zuständigen Bundesoberbehörde i. S. v. § 77 AMG die Person des Datentreuhänders anzuzeigen, damit die Inspektoren ggf. Kontakt zu dem Datentreuhänder aufnehmen können, wenn dies zur Überwachung der ordnungsgemäßen Durchführung notwendig ist. Dies gilt jedenfalls dann, wenn dem Datentreuhänder im Rahmen etwa der Meldepflichten, des Genehmigungsverfahrens oder aber späterer Verfahrensänderungen – sog. „substantial admendments“ – eine zentrale Rolle zukommen soll. Dabei ist jeweils die konkrete Ausgestaltung der Einbindung des Datentreuhänders in das Organisationssystem der klinischen Prüfung maßgeblich. Insbesondere in Anbetracht dessen, dass ihm aufgrund seiner Aufgabe zur Reidentifikation von Patientendaten im Entblindungsverfahren nach § 6 GCP-V eine wichtige Position zukommen wird, kann sich bspw. eine Modifizierung der Verfahrensweise des Datentreuhänders durchaus als wesentliche organisatorische Änderung darstellen. Denn diese Änderung wird in der Regel die nach GCP-V

[128] Punkt 5 der Stellungnahme des Wissenschaftlichen Beirates der Bundesärztekammer zur Wahrung der ärztlichen Schweigepflicht und des Datenschutzes in der medizinischen Forschung, DÄBl. 1989, C-1744).

notwendige Entblindung beeinflussen. Insofern erscheint es auch nicht abwegig, das Datentreuhänderverfahren unter § 10 GCP-V, insbesondere Abs. 1 Nr. 1 und 3, zu fassen. Gemäß § 10 Abs. 1 Nr. 1 und 3 GCP-V darf der Sponsor Änderungen einer von der zuständigen Bundesoberbehörde genehmigten oder von der zuständigen Ethik-Kommission zustimmend bewerteten klinischen Prüfung, die geeignet sind, sich auf die Sicherheit der betroffenen Personen auszuwirken (Nr. 1) oder die **Art der Leitung oder Durchführung der Studie wesentlich zu verändern** (Nr. 3), nur vornehmen, wenn diese Änderungen von der zuständigen Ethik-Kommission zustimmend bewertet wurden, soweit sie die Anlagen und Unterlagen nach § 7 Abs. 2 oder 3 betreffen, und wenn sie von der zuständigen Bundesoberbehörde genehmigt wurden, soweit sie die Angaben und Unterlagen nach § 7 Abs. 2 oder 4 betreffen. Die zustimmende Bewertung ist bei der zuständigen Ethik-Kommission, die Genehmigung ist bei der zuständigen Bundesoberbehörde zu beantragen. Der Antrag muss begründet werden. Bei entsprechender Einbindung des Datentreuhänders in den Organisationsablauf der klinischen Prüfung sollten daher die dargestellten Anforderungen des § 10 GCP-V sicherheitshalber eingehalten und entsprechende Anträge bei der zuständigen Bundesoberbehörde bzw. Ethik-Kommission gestellt werden.

Bei der Einbindung eines Datentreuhänders muss zudem für alle Beteiligten sichergestellt werden, dass in den erlaubten Fällen die **Reidentifikation** durchführbar ist. Ein solcher Fall ist der bereits angesprochene § 40 Abs. 2a Nr. 1a AMG **(behördliche Überwachung und Monitoring)**. Im Übrigen kann ein Interesse an dem Zugriff auf Patientendaten wegen Prüfungen zur **Qualitätssicherung** bestehen; da nach § 28 AMG hierzu auch ein Zugriff auf die Originalunterlagen erlaubt sein muss.[129] Zudem dürfte eine Reidentifikation etwa dann angezeigt sein, wenn eine nicht anders abwendbare **Gefahr** für den Patienten besteht (Notstandssituation im Sinne von § 34 StGB). In diesem Fall darf die Reidentifikation aber nur im notwendigen Maße erfolgen, d.h. im Regelfall entweder gegenüber dem Patienten selbst oder den behandelnden Ärzten (soweit diese nicht ohnehin den Code des Patienten kennen, da sie zu den Prüfärzten gehören). Da der Sponsor oder externe Forscher den Patienten nicht behandelt, besteht bei ihnen regelmäßig kein Interesse, über die Person des Patienten Bescheid zu wissen. Sollten Sponsoren klinischer Prüfungen oder externe Forscher wegen erkannter Gefahrensituationen für die betroffene Person einen Reidentifikationsbedarf sehen dürfte es daher reichen, wenn sie den Datentreuhänder benachrichtigen, der seinerseits die Reidentifikation und die erforderlichen Mitteilungen (an die behandelnden Ärzte) durchführt.

Sollen die Daten aus der klinischen Forschung einem **Kompetenznetz bzw. einer medizinischen Sammlung**, die u. a. Forschungszwecke verfolgt, zugeführt werden – in die

[129] Bundestags-Drucks. 16/5374 - betr. Technikfolgenabschätzung bei Biobanken -, S. 78

Nutzung zu diesen Zwecken hat die betroffene Person selbstverständlich vorher einzuwilligen – können sich aus der Analyse der Forschungsdaten **mögliche neue und bessere Behandlungsoptionen**, auch Optionen auf Teilnahme an weiteren klinischen Studien ergeben, die man dem Patienten mitteilen sollte.[130] Möglicherweise kann hieraus ein Interesse entstehen, eine Reidentifikation vorzunehmen und eine Mitteilung vorzunehmen. Allerdings ist es im Recht der klinischen Prüfungen derzeit gesetzlich nicht geregelt, eine Reidentifikation in diesen Fällen vorzunehmen. Zudem fehlen gesetzliche Rahmenbedingungen, so dass die Frage solcher Rückmeldungsmöglichkeiten anders geklärt werden müsste, bspw. im Rahmen der Patienteneinwilligung. Überdies betrifft die Frage der Reidentifikation wegen verbesserten Behandlungsoptionen eher den Fragenkreis der Rückmeldung auf Auskunftsersuchen der betroffenen Person oder ihres Arztes und wird daher unten unter 6.2. behandelt werden.

Für den beschrieben Datenfluss und notwendigen und erlaubten Fälle der Reidentifikation sollte die Mitwirkung des Datentreuhänders unter allen Beteiligten des klinischen Prüfung (Sponsoren, Prüfärzte, betroffene Personen i. S. v. § 3 Abs. 2a GCP-V) **vertraglich abgesichert** werden.

2.9.6 Meldepflichten bei klinischen Prüfungen

a) Normadressat und Inhalt der Meldepflichten

Für die in der GCP-V normierten Meldepflichten sind als Normadressaten Prüfer (§ 12 CGP-V) und Sponsoren (§ 13 GCP-V) genannt.

Die Meldepflichten des **Prüfarztes** gem. § 12 Abs.4 und 6 GCP-V sind folgende:

> Der Prüfer hat den Sponsor unverzüglich über das Auftreten eines schwerwiegenden unerwünschten Ereignisses, ausgenommen Ereignisse, über die laut Prüfplan oder Prüferinformation nicht unverzüglich berichtet werden muss, zu unterrichten und ihm anschließend einen ausführlichen schriftlichen Bericht zu übermitteln. Personenbezogene Daten sind vor ihrer Übermittlung unter Verwendung des Identifizierungscodes der betroffenen Person zu pseudonymisieren.
>
> Im Fall des Todes einer betroffenen Person übermittelt der Prüfer der zuständigen Ethik-Kommission, bei multizentrischen Studien auch der beteiligten Ethik-Kommission, der zuständigen Bundesoberbehörde sowie dem Sponsor alle für die Erfüllung ihrer Aufgaben erforderlichen zusätzlichen Auskünfte. Personenbezogene Daten sind vor ihrer Übermittlung unter Verwendung des Identifizierungscodes der betroffenen Person zu pseudonymisieren. (lt. FAQ des BfArM jedoch nur auf Anfrage der EK oder BOB.)

[130] siehe Bundestags-Drucks. 16/5374, S. 76; dort als eines der Gründe genannt, die ein pseudonymisierte statt eine anonymisierte Nutzung von Daten bei medizinischen Datensammlungen erforderlich machen können.

Die Meldepflichten des Sponsors sind gem. § 13 Abs. 1, 2 und 3 GCP-V folgende:

> Der Sponsor hat alle ihm von den Prüfern mitgeteilten unerwünschten Ereignisse ausführlich zu dokumentieren. Diese Aufzeichnungen werden der zuständigen Bundesoberbehörde und den zuständigen Behörden anderer Mitgliedstaaten der Europäischen Union und anderer Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum, in deren Hoheitsgebiet die klinische Prüfung durchgeführt wird, auf Anforderung übermittelt. Personenbezogene Daten sind vor ihrer Übermittlung unter Verwendung des Identifizierungscodes der betroffenen Person zu pseudonymisieren.
>
> Der Sponsor hat über jeden ihm bekannt gewordenen Verdachtsfall einer unerwarteten schwerwiegenden Nebenwirkung unverzüglich, spätestens aber innerhalb von 15 Tagen nach Bekanntwerden, die zuständige Ethik-Kommission, die zuständige Bundesoberbehörde und die zuständigen Behörden anderer Mitgliedstaaten der Europäischen Union und anderer Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum, in deren Hoheitsgebiet die klinische Prüfung durchgeführt wird, sowie die an der klinischen Prüfung beteiligten Prüfer zu unterrichten. Personenbezogene Daten sind vor ihrer Übermittlung unter Verwendung des Identifizierungscodes der betroffenen Person zu pseudonymisieren.
>
> Der Sponsor hat bei jedem ihm bekannt gewordenen Verdachtsfall einer unerwarteten schwerwiegenden Nebenwirkung, die zu einem Todesfall geführt hat oder lebensbedrohlich ist, unverzüglich, spätestens aber innerhalb von sieben Tagen nach Bekanntwerden, der zuständigen Ethik-Kommission, der zuständigen Bundesoberbehörde und den zuständigen Behörden anderer Mitgliedstaaten der Europäischen Union und anderer Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum, in deren Hoheitsgebiet die klinische Prüfung durchgeführt wird, sowie den an der Prüfung beteiligten Prüfern alle für die Bewertung wichtigen Informationen und innerhalb von höchstens acht weiteren Tagen die weiteren relevanten Informationen zu übermitteln. Personenbezogene Daten sind vor ihrer Übermittlung unter Verwendung des Identifizierungscodes der betroffenen Person zu pseudonymisieren.

Eine Pflicht zur **elektronischen Anzeige** kann sich gem. § 2 Abs.1 AMG-AV (BGBl I 2005, 2775) ergeben, wobei das entsprechende Formulars (http://www.cioms.ch/cioms.pdf) zu verwenden ist.

b) Übertragbarkeit von Meldepflichten auf Datentreuhänder?

Da Sponsor und Prüfer die Adressaten der Meldepflichten sind, könnte der Datentreuhänder allenfalls in einer Weise eingebunden werden, dass die entsprechenden Pflichten auf ihn delegiert werden. Gem. Art. 7 Abs. 1 Satz 1 der Richtlinie 2005/28/EG ist es dem Sponsor gestattet, seine prüfungsbezogenen Verantwortlichkeiten ganz oder teilweise an eine Einzelperson, ein Unternehmen, eine Institution oder eine Einrichtung zu delegieren. Gem. Art. 7 Abs. 1 Satz 2 ist der Sponsor aber nach wie vor dafür verantwortlich, dass sowohl die Durchführungen der Prüfungen als auch die aus diesen Prüfungen hervorgehenden abschließenden Daten den Anforderungen der Richtlinie 2001/20/EG sowie der Richtlinie 2005/28/EG entsprechen. Der **Sponsor** kann also Aufgaben delegieren, sich aber nicht von der **Gesamtverantwortlichkeit** befreien. Ihn trifft weiterhin eine generelle Gewährleistungspflicht, dass die bestehenden Regeln eingehalten werden.

Für den **Prüfarzt** besteht nach ICH-GCP/135/95 und Entwurf Eudralex-Leitlinien ebenfalls die Möglichkeit zur Delegation von Pflichten, doch bleibt auch er **Gesamtverantwortlicher**.[131] Insofern bleibt es dabei, dass eine vollständige Verschiebung der Verantwortlichkeiten in Richtung des Datentreuhänders durch vertragliche Vereinbarungen nicht erfolgen kann. Die gesetzlichen Vorschriften bleiben trotz interner Delegationsmöglichkeiten zwingendes Recht für den Prüfarzt.

2.9.7 Antragsstellung für klinische Prüfungen

Die **Antragstellung** für die klinische Prüfung erfolgt bei der nach § 77 AMG zuständigen Bundesoberbehörde und der nach § 42 Abs. 1 AMG zuständigen Ethikkommission. Die Antragstellung hat durch den Sponsor zu geschehen.

Bei der Antragstellung ist aber auch der datenschutzrechtliche Aspekt von Bedeutung, weshalb eine Einbindung des Datentreuhänders möglich wäre. Gem. § 7 Abs. 2 Nr. 15 GCP-V muss dem Antrag an die zuständige Ethik-Kommission und dem Antrag an die zuständige Bundesoberbehörde vom Antragsteller unter anderem die Bestätigung beigefügt werden, dass betroffene Personen über die Weitergabe ihrer pseudonymisierten Daten im Rahmen der Dokumentations- und Mitteilungspflichten nach § 12 und § 13 an die dort genannten Empfänger aufgeklärt werden; diese muss eine Erklärung enthalten, dass betroffene Personen, die der Weitergabe nicht zustimmen, nicht in die klinische Prüfung eingeschlossen werden. Des Weiteren ist der zuständigen Ethikkommission vom Sponsor u.a. eine **Erklärung zur Einhaltung des Datenschutzes** beizufügen, § 7 Abs. 3 Nr. 15 GCP-V.

Bei diesen Unterlagen könnte auch eine entsprechende Erklärung des Datentreuhänders über die Einhaltung des Datenschutzes bei der klinischen Prüfung angefügt werden.

2.9.8 Kennzeichnung von Prüfpräparaten

Da bei der **Kennzeichnung von Prüfpräparaten** bei klinischen Prüfungen u.a. der Schutz der betroffenen Person zu beachten ist, § 5 Abs. 1 CGP-V, müssen die Prüfpräparate u.a. mit dem **Identifizierungscode** der betroffenen Person gekennzeichnet sein (§ 5 Abs. 2 Nr. 12 GCP-V). Diese Prozedur ändert sich nicht dadurch, dass ein Datentreuhänder eingeschaltet wird. Allerdings sollte der Identifizierungscode auf den Prüfpräparaten dem Datentreuhänder bekannt sein, damit

[131] „The documents to be retained by the investigator may be stored in commercial archives. This may also be an option (in some Member States) for source data, when the hospital/institution is unable to retain patients’ trial records, relating to clinical trials, for a sufficient length of time”.

er eine optimale Identitätsverwaltung bei der Verwaltung von Patientenlisten bei der klinischen Prüfung vornehmen kann.

2.9.9 Dokumentations- und Aufbewahrungspflichten

Es ergeben sich **Dokumentationspflichten** für den Sponsor gem. § 13 Abs. 9 und 10 GCP-V:

> Der Sponsor übermittelt der zuständigen Bundesoberbehörde und der zuständigen Ethik-Kommission innerhalb eines Jahres nach Beendigung der klinischen Prüfung eine Zusammenfassung des Berichts über die klinische Prüfung, der alle wesentlichen Ergebnisse der klinischen Prüfung abdeckt.
>
> Der Sponsor stellt sicher, dass die wesentlichen Unterlagen der klinischen Prüfung einschließlich der Prüfbögen nach der Beendigung oder dem Abbruch der Prüfung mindestens zehn Jahre aufbewahrt werden. Andere Vorschriften zur Aufbewahrung von medizinischen Unterlagen bleiben unberührt.

Auch diese Dokumentations- und Aufbewahrungspflichten könnten auf Wunsch des Sponsors vertraglich teilweise auf den Datentreuhänder delegiert werden, so lange der Sponsor seine Gesamtverantwortlichkeit behält. Insbesondere kann ein Bedürfnis bestehen, den Datentreuhänder bei der Erstellung des Abschlussberichtes der klinischen Forschung hinzu zu ziehen. Zu den Funktionen eines Datentreuhänders kann es gerade gehören, Forschungsberichte vorzulegen[132] oder gewünschte Auswertungen durchzuführen[133].

Unabhängig von der grundsätzlichen Zulässigkeit der Hinzuziehung eines externen Dienstleisters zur Aufbewahrung nach den relevanten europarechtlichen Vorgaben gilt es, daneben die **Datenschutzkonformität** sicher zu stellen. Der besondere Schutzbedarf gerade von personenbezogenen Gesundheitsdaten wurde von der Rechtsprechung – auch mit Blick auf Outsourcing-Verfahren – betont.[134] Die datenschutzrechtliche Problematik der Auslagerung von Funktionsbereichen im Bereich der Krankenversorgung wurde auch bereits mehrfach von den Datenschutzbeauftragten von Bund und Ländern thematisiert.[135] Insofern bedarf es stets einer

---

[132] Bundestags-Drucks. 16/5374 (betr. Technikfolgenabschätzung bei Biobanken), S. 11

[133] Bizer, DuD, 1999, 392, 394

[134] Vgl. BayVerfGH, Entscheidung vom 6. April 1989 – Akz.: Vf. 2 VII – 87 = CR 1989, 530 (zur Zulässigkeit des gesetzlichen Verbots, medizinische Daten außerhalb des Krankenhauses durch private Unternehmen verfilmen zu lassen); BVerfG, Beschluss vom 25. September 1990. Akz: 1 BvR 1555/87 = CR 1991, 296 (ebenfalls zum gesetzlichen Verbot der externen Mikroverfilmung von Patientendaten) und zuletzt OLG Düsseldorf, Urteil vom 20. August 2006 – Akz. 20 U 139/95, CR 1997, S. 536 (zur externen Archivierung von Patientendaten).

[135] Vgl. bereits die Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997, den 26. Tätigkeitsbericht (1998) des Hessischen

genauen Prüfung der einzelnen Arbeitsaufträge dahingehend, ob sie für die Beauftragung eines Datentreuhänders geeignet sind.

Im Übrigen ist zu gewährleisten, dass das vertragliche Delegieren von Dokumentations- und Aufbewahrungsleistungen nicht die **Verfügbarkeit** beeinträchtigt. Durch den Bundesgerichtshof wurde in mehreren Entscheidungen betont, dass es eine wesentliche Pflicht des Krankenhausträgers ist, jederzeit positive Kenntnis über den Verbleib von Krankenunterlagen zu haben.[136] Mit der Notwendigkeit einer Kenntnis über den Verbleib von Unterlagen korrespondiert die grundsätzliche Pflicht von Sponsor und Prüfarzt, auch bei einer Aufbewahrung von Unterlagen bei einem Datentreuhänder die jederzeitige Verfügbarkeit sicherzustellen. Diesen beiden Aspekten ist auch bei der Hinzuziehung eines Datentreuhänders durch organisatorische Maßnahmen zu entsprechen.

Der Anhang 1 der Richtlinie 2001/83/EG benennt wissenschaftliche und technische Vorgaben für die Erstellung des Zulassungsdossiers, welches bei Beantragung der Zulassung eines Humanarzneimittels für den europäischen Gemeinschaftsmarkt bei der Zulassungsbehörde einzureichen ist. In Modul 5 (Berichte über klinische Studien) werden im Anhang 1 auch Vorgaben für Format, Präsentation und Aufbewahrungsfristen für Berichte über klinische Studien formuliert. Mit Wirkung zum 1. Juli 2003 wurde der Anhang 1 der Richtlinie 2001/83/EG durch die Richtlinie 2003/63/EG vom 25. Juni 2003 geändert.[137] Der überarbeitete Anhang 1 enthält weiterhin im Modul 5 wesentliche **Dokumentationsvorgaben** an den Zulassungsinhaber mit Blick auf die zuvor durchgeführte klinische Prüfung. Unter Punkt 5.2 wird bestimmt, dass die **Zulassungsinhaber** dafür Sorge zu tragen haben, dass die wesentlichen Dokumente für die klinische Prüfung (einschließlich Prüfbögen) von den Eigentümern der Daten für eine bestimmte Zeit aufbewahrt werden. Für die medizinische Akte des Prüfungsteilnehmers gilt diese Regelung nicht. Als Aufbewahrungsdauer gibt Richtlinie 2003/63/EG für die erfassten Unterlagen vor: (1) mindestens **15 Jahre** nach Abschluss oder Abbruch der Prüfung; (2) oder mindestens **2 Jahre** nach Erteilung der letzten Zulassung in der Europäischen Gemeinschaft, bis keine

---

Landesdatenschutzbeauftragten, Punkt 7.1.4 (Auslagerung von Funktionsbereichen); den Tätigkeitsbericht 2005 des Berliner Beauftragten für Datenschutz und Informationsfreiheit, Punkt 4.5. 1, S. 113 f. (Outsourcing im Krankenhaus), online abrufbar unter www.datenschutz-berlin.de sowie die Orientierungshilfe „Archivierung von Krankenunterlagen des Krankenhauses und Outsourcing“, S. 11 ff. der Landesbeauftragten für Datenschutz und Informationsfreiheit, online abrufbar unter www.ldi.nrw.de.

[136] BGH, Urteil vom 21. November 1995, NJW 1996, 779 (781); Urteil vom 13. Februar 1996, NJW 1996, 1589 (1590).

[137] ABl. EG Nr. L 159 v. 27.06.2003.

Zulassungsanträge in der Europäischen Gemeinschaft mehr anhängig sind oder in Aussicht stehen; oder (3) mindestens **2 Jahre** nach dem formellen Abbruch der klinischen Entwicklung des Prüfpräparates.

An den **Sponsor** bzw. die Personen, in deren Besitz sich die Daten befinden, richtet sich die in der Richtlinie 2003/63/EG normierte Pflicht, alle Versuchsunterlagen für die **gesamte Dauer der Zulassung** des Arzneimittels aufzubewahren. Als Bestandteile der Versuchsunterlagen werden genannt: der Prüfplan mit der Begründung, Zielsetzung, statistischen Konzeption und Methodik der Prüfung und den Bedingungen, unter denen sie durchgeführt und geleitet werden; ausführliche Angaben zum Prüfpräparat, dem Referenzarzneimittel und / oder den verwendeten Placebos; die Standardarbeitsanweisungen (SOP); sämtliche schriftlichen Stellungnahmen zum Prüfplan und zu den Verfahren; die Prüferinformation; die Prüfbögen für jede Versuchsperson; den Abschlussbericht und ggf. Auditbescheinigungen.

Konkrete an den Sponsor gerichtete Pflichten benennt ebenfalls Art. 17 Richtlinie 2005/28/EG. Auch der Sponsor einer klinischen Studie muss die wesentlichen Dokumente über alle klinischen Prüfungen **nach Abschluss der Prüfung** mindesten **5 Jahre** aufbewahren. Auch er ist verpflichtet, die Dokumente länger aufzubewahren, wenn dies aufgrund anderer geltender Anforderungen oder aufgrund einer Vereinbarung zwischen dem Sponsor und dem Prüfer erforderlich ist. Den Pflichten des Sponsors entsprechen auch die verfahrenstechnischen Anforderungen, die bereits für den Sponsor formuliert wurden. Auch der Sponsor hat die wesentlichen Dokumente so aufzubewahren, dass sie den zuständigen Behörden auf Verlangen **rasch bereitgestellt** werden können.

Gemäß der Richtlinie 2003/63/EG Anhang I 5.2.c.[138] muss der Sponsor bzw. andere Personen, in deren sich die Daten befinden, alle Versuchsunterlagen **solange aufbewahren, wie das Arzneimittel zugelassen ist**. Nachdem keine Zulassung für das Arzneimittel mehr besteht, ist der Abschlussbericht vom Sponsor oder von anderen Personen, in deren Besitz er sich befindet, weitere **fünf Jahre** lang aufzubewahren.

Gem. § 13 Abs. 1 GCP-VO hat der Sponsor zudem alle ihm vom Prüfer mitgeteilten, im Rahmen der Studiendurchführung aufgetretenen unerwünschten Ereignisse ausführlich zu dokumentieren. Gem. § 13 Abs. 10 GCP-VO hat der Sponsor zudem sicherzustellen, dass die **wesentlichen**

[138] In das nationale Recht implementiert durch die Zweite Allgemeine Verwaltungsvorschrift zur Änderung der Allgemeinen Verwaltungsvorschrift zur Anwendung der Arzneimittelprüfrichtlinien vom 11.10.2004 (BAnz. Nr. 197 vom 16.10.2004).

Unterlagen der klinischen Prüfung einschließlich der Prüfbögen nach der Beendigung oder dem Abbruch der Prüfung mindestens **10 Jahre** aufbewahrt werden.

Was **„wesentliche Unterlagen“** sind, bestimmt die GCP-VO nicht. Allerdings kann anhand des Zwecks der Regelung der Umfang der aufzubewahrenden Unterlagen umrissen werden. Die „wesentlichen Unterlagen“ sollen einzeln oder zusammen eine Bewertung der Durchführung der klinischen Prüfung sowie der Qualität der erhobenen Daten ermöglichen. Die vollständigen Unterlagen sollen die Einhaltung der Guten klinischen Praxis und aller geltenden gesetzlichen Bestimmungen durch den Prüfer, den Sponsor und den Monitor belegen.[139] Insoweit werden auch für den Umfang der durch den Sponsor aufzubewahrenden Unterlagen die ICH-GCP-Leitlininie 8 („Essential documents for the conduct of a clinical trial“) sowie der Entwurf von Empfehlungen für den **Inhalt des Trial Master Files** und dessen Aufbewahrung in EUDRALEX Kapitel 5 (Additional Information) relevant. Im erheblichen Umfang entsprechen die vom Sponsor zu aufzubewahrenden Unterlagen damit denen des Prüfers.[140]

> **Gruppe 1** (Dokumente, die bereits vor Beginn der Durchführung der klinischen Prüfung vorliegen müssen): Prüferinformationen; unterzeichneter Prüfplan und Prüfänderungen (soweit vorhanden) sowie Musterprüfbogen; sonstige den Prüfungsteilnehmern übermittelten Informationen; über die finanziellen Aspekte der Prüfung; Versicherungsnachweise; die unterzeichneten Vereinbarungen zwischen den an der Prüfung beteiligten Parteien, um Übereinstimmung zu dokumentieren; Dokumentation der datierten Zustimmung der Ethik-Kommission zu den bei ihr eingereichten Unterlagen; Dokumentation der Zusammensetzung der Ethik-Kommission; Dokumentation der Genehmigung / Anzeige des Prüfplans bei der zuständigen Behörde (falls erforderlich); Lebensläufe und ggf. weitere Befähigungsnachweise (Qualifikation) der Prüfer und Personen, an die Prüfaufgaben delegiert werden; Übersicht der Normalwerte / Bereiche für die im Prüfplan genannten medizinischen Verfahren, technischen Verfahren und Laborverfahren sowie sonstiger Tests; Zertifizierungsnachweise / Qualitätsnachweise für die in der Prüfung eingesetzten medizinischen Verfahren, technischen Verfahren und Laborverfahren; Muster der für die Kennzeichnung der Prüfpräparate-Behälter bestimmten Etiketten; Handhabungshinweise für die in der Prüfung verwendeten Prüfpräparate und sonstiger verwendeter Materialien (soweit nicht schon im Prüfplan genannt); Versandunterlagen für die Prüfpräparate; Analysezertifikate der Prüfpräparate (bzgl. Identität/Reinheit/Stärke); Dokumentation des Decodierungsverfahren bei verblindeten klinischen Prüfungen; das Originaldokument der Randomisierungsliste; Monitoringberichte für den Zeitraum vor und zu Beginn der klinischen Prüfung.
>
> **Gruppe 2** (Dokumente, die während der Durchführung der klinischen Prüfung zu den Akten zu nehmen sind): das Update der Prüferinformationen; alle überarbeiteten Fassungen von Prüfplan und Prüfbogen, des Formblattes zur Einwilligungserklärung, der (ggf.) geschalteten (Werbe-)Anzeigen, sowie alle schriftlichen Informationen der Prüfungsteilnehmer; Dokumentation der datierten Zustimmung der Ethik-Kommission zu den bei ihr eingereichten geänderten / aktualisierten Unterlagen; Dokumentation der Genehmigung / Anzeige des geänderten / aktualisierten Prüfplans bei der zuständigen Behörde (falls erforderlich); Lebensläufe und ggf.

[139] ICH-GCP Leitlinie 8 (Essential documents for the conduct of a clinical trial), Einleitung.

[140] Siehe auch *Schwarz*, Klinische Prüfungen von Arzneimitteln und Medizinprodukten, S. 234 ff.

weitere Befähigungsnachweise (Qualifikation) der neu in die Prüfung eingetretenen Prüfer und Personen, an die Prüfaufgaben delegiert werden; aktualisierte Übersicht der Normalwerte / Bereiche für die im Prüfplan genannten medizinischen Verfahren, technischen Verfahren und Laborverfahren sowie sonstiger Tests; aktualisierte Zertifizierungsnachweise / Qualitätsnachweise für die in der Prüfung eingesetzten medizinischen Verfahren, technischen Verfahren und Laborverfahren; Versandunterlagen für die Prüfpräparate; Analysezertifikate für neue Chargen des Prüfpräparates; Dokumentation des Monitorings / Besuche des Monitors; Dokumentation sonstiger Kommunikation außerhalb von Besuchen vor Ort (Briefe, Besprechungs- und Telefonnotizen); originale „Quell-Dokumente“ (z.B. Nachweis der Existenz der Prüfungsteilnehmer etc.); Unterschriebene, datierte und vollständige Prüfbögen (Original); Dokumentation von Korrekturen im Prüfplan (Original); Dokumentation der Benachrichtigungen des Sponsors bei schwerwiegenden unerwünschten Ereignissen und der damit verbundenen Berichten; Dokumentation der Unterrichtung der zuständigen Behörde / der Ethik-Kommission über unerwartete und schwerwiegende Reaktionen sowie sonstiger Sicherheitsinformationen durch den Sponsor / den Prüfer; Dokumentation der Benachrichtigung des Prüfers durch den Sponsor über sicherheitsrelevante Informationen; Dokumentation des Zwischen- oder Jahresberichtes für die zuständigen Behörden und die Ethik-Kommission (falls erforderlich); Liste der Prüfungsteilnehmer (Probanten), mit denen vor der Prüfung ein Eignungstest durchgeführt wurde; Nachweis der Verwendung der Prüfpräparate; vollständiges Unterschriftenblatt sämtlicher Personen, die berechtigt sind, im Rahmen der Prüfung auf Prüfbögen Eintragungen oder Korrekturen vorzunehmen; Verzeichnis der aufbewahrten Körperflüssigkeiten und / oder Gewebeproben.

Gruppe 3 (Dokumente, die nach Abschluss oder Abbruch der klinischen Prüfung zu den Akten genommen werden sollten): vollständiger Verwendungsnachweis der während der klinischen Prüfung verwandten Prüfpräparate; Dokumentation der ordnungsgemäßen Entsorgung von nicht genutzten Prüfpräparaten; Audit-Zertifikat (falls ein Audit durchgeführt wurde); finaler Monitoringbericht bei Beendigung der klinischen Prüfung (insbesondere über Vorliegen der wesentlichen Unterlagen); Dokumentation vorgenommener Entblindungen (an den Sponsor zu übergeben); klinischer Prüfungsbericht zur Dokumentation der Ergebnisse und ihrer Interpretation.

F2.10 Welche Anforderungen werden an einen Dienstleister grundsätzlich und an sein administratives Personal (Wartungstechniker) bezüglich Ausbildung und Schweigepflicht gestellt und wie überprüft? Wie kann die Vertraulichkeit eines Dienstleisters gewährleistet werden?

Bislang fehlen gesetzliche Regelungen darüber, wie die fachliche Eignung und die Vertrauenswürdigkeit des Datentreuhänders sichergestellt werden können.

Wegen der Vertraulichkeit, die der Datentreuhänder erfüllen muss, wird jedoch vielfach gefordert, dass er bestimmten **Berufsgruppen** zugehört. So heißt es etwa in der Stellungnahme des Bundestages zur Technikfolgenabschätzung zu Biobanken[141]:

[141] Bundestags-Drucks. 16/5374, S. 103

> „Die damit durch den Datentreuhänder wahrgenommene Funktion eines „vertrauenswürdigen Dritten“ kann noch verstärkt werden, wenn dieser einer Berufsgruppe angehört, die gesetzlich zur Verschwiegenheit verpflichtet ist und deren Unterlagen und Daten einem Beschlagnahmeschutz unterliegen (Beispiele: Rechtsanwälte, Notare). Datentreuhänder werden bereits von einigen medizinischen Kompetenznetzen eingesetzt.“

Dennoch ist zu berücksichtigen, dass ein umfassender Beschlagnahmeschutz über einen Notar als Treuhänder nach der gegenwärtigen Ausgestaltung der §§ 53 f., 97 StPO, § 203 StGB nicht zu erreichen sein wird[142]. Allerdings sind Durchsuchung und Beschlagnahme von Datenträgern bei Berufsgeheimnisträgern, wie bereits dargestellt, besonders restriktiven Anforderungen bezüglich ihrer Verhältnismäßigkeit unterworfen. Dies gilt insbesondere unter Berücksichtigung von Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Zudem darf in die beim Notar beschlagnahmten Unterlagen grundsätzlich keine Einsicht für Dritte gewährt werden.[143]

Art. 7 des Bayerischen Krebsregistergesetzes[144] fordert dementsprechend etwa, dass die Vertrauensstelle „unter ärztlicher Leitung steht“. Ein berühmtes Beispiel für die **notarielle** Datentreuhänderschaft ist das Kompetenznetzwerk Parkinson (GEPARD).[145] Diese Berufsgruppen sind bereits gesetzlich zur Vertraulichkeit verpflichtet, auch wenn ein umfassender Beschlagnahmeschutz in diesem Zusammenhang wohl nicht gewährleistet werden kann. Denn die grundsätzliche Vertraulichkeit der entsprechenden Berufsgruppe, z.B. der der Notare, im Verhältnis zu sonstigen Personen ist schon für sich gesehen erheblich. Gleichwohl werden an die Zulässigkeit von Durchsuchung und Beschlagnahme besonders strenge Anforderungen gestellt. Deshalb kann die Vertrauenswürdigkeit des Datentreuhänders trotz fehlenden Beschlagnahmeschutzes durch die Beauftragung bspw. eines Notars gesteigert werden.

Es spricht im Übrigen nichts dagegen, die Vertraulichkeit zusätzlich durch **Vertraulichkeitsvereinbarungen** -die auf die auf **privatvertraglicher** Basis jederzeit zwischen allen privaten Personen abgeschlossen werden können – zu bekräftigen[146]. Es käme hierbei darauf an, wie sich die jeweilige Interessenlage darstellt. Der Datentreuhänder schuldet grundsätzlich in erster Linie den betroffenen Personen (bei klinischen Prüfungen: betroffene Person gem. § 3 Abs. 2a GCP-V) eine Vertraulichkeit. Das Maß der Vertraulichkeit wird in diesem Fall aber auch bereits

---

[142] Vgl. oben S. 23.

[143] Kanzleiter in Schippel/Bracker, BNotO, § 18, Rdnr. 62.

[144] (G. v. 25.07.2000, GVBl S. 274, zuletzt geändert durch G. vom 24.12.2005, GVBl. S. 652):

[145] Dargestellt in Bundestags-Drucks. 16/5374, S. 21

[146] Vgl. auch Bizer, DuD 1999, 392, 394: „Die Vertrauenswürdigkeit des Datentreuhänders kann durch vertragliche Abreden, aber auch durch öffentlich-rechtliche Bestimmungen abgesichert werden.“

durch die geltenden Gesetze und die Patienteneinwilligung geregelt. Prinzipiell darf der Datentreuhänder danach gegenüber Unbefugten keine Reidentifikation durchführen. Es kann sich anbieten, zwischen Sponsoren und Prüfärzten sowie Forschern, die ein ggf. zu errichtendes Kompetenznetzwerk oder eine medizinische Sammlung nutzen, die Vertraulichkeit in weiteren Punkten zu regeln.

Zusätzliche Anforderungen an die Qualifikation eines Datentreuhänders können sich stellen, wenn man die Anforderungen für einen **Datenschutzbeauftragten** als eine Orientierungshilfe nimmt. Denn Datenschutzbeauftragte zeichnen sich u.a. durch eine Kontroll- und Vermittlungsfunktion aus,[147] womit sie eine Gemeinsamkeit zu Datentreuhändern aufweisen. Zum Datenschutzbeauftragten darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Sachkunde besitzt (§ 4f Abs. 3 BDSG). Dies umfasst **rechtliche, organisatorische und technische** Kenntnisse. Gleichwohl gibt es auch für einen Datenschutzbeauftragten kein festes Anforderungsprofil.[148]

Was die rechtlichen Anforderungen anbelangt, so ist aber zu fordern, dass rein summarische Kenntnisse nicht ausreichen und der Datenschutzbeauftragte vielmehr über genügend rechtliche Kenntnisse verfügen muss, um Hintergrund, Anforderungen und Ziel der datenschutzrelevanten rechtlichen Regelungen erkennen und so auch die Konsequenzen für die verantwortliche Stelle ausmachen zu können.[149] Der Datentreuhänder sollte in diesem Sinne ebenfalls ausreichende rechtliche Kenntnisse haben.

Die organisatorische Kompetenz verlangt des Weiteren mindestens, dass der Datenschutzbeauftragte in der Lage ist, organisatorische Zusammenhänge zu definieren, was wiederum die Kenntnis der Funktionszusammenhänge bei der verantwortlichen Stelle voraussetzt.[150] Bei der Erstellung rechtlicher und organisatorsicher Anforderungen an einen Datentreuhänder dürfte im vorliegenden Fall ebenso zu fordern sein, dass die betreffende Person über eine hinreichende Kenntnis bezüglich aller rechtlichen Rahmenbedingungen der medizinischen Forschung und des medizinischen Behandlungsverhältnisses, sowie des allgemeinen und besonderen Datenschutzrechts verfügt. Von Vorteil wäre, wenn die Person selbst eine gewisse Erfahrung in der medizinischen Forschung aufwiese, um die Funktionszusammenhänge bei den Beteiligten besser verstehen zu können. Die diesbezüglichen Anforderungen dürfen aber nicht überspannt werden. Dies gilt insbesondere im Hinblick darauf, dass bspw. ein Notar nur in

[147] Simitis, Kommentar zum BDSG, 6. Aufl., § 4f, Rn. 91

[148] Simitis, Kommentar zum BDSG, 6. Aufl., § 4f, Rn. 84

[149] Simitis, Kommentar zum BDSG, 6. Aufl., § 4f, Rn. 88

[150] Simitis, Kommentar zum BDSG, 6. Aufl., § 4f, Rn. 91

seltenen Fällen bereits mit dem Bereich der medizinischen Forschung in Berührung gekommen sein dürfte. Insofern ist die „Forschungserfahrung“ im medizinischen Sinne nicht als zwingende Voraussetzung für die Eignung einer Person als Datentreuhänder anzusehen. Dieses Kriterium ist vielmehr dahingehend zu verstehen und auszulegen, dass er sich zumindest sowohl mit den rechtlichen Rahmenbedingungen der medizinischen Forschung als auch denen des Behandlungsverhältnisses vertraut gemacht haben muss. Zwar bestimmt Art. 2 Abs. 2 der Richtlinie 2005/28/EG über die Durchführung klinischer Prüfungen, dass jede an der Durchführung einer klinischen Prüfung beteiligte Person durch Aus- und Weiterbildung sowie berufliche Erfahrung für die Ausführung ihrer jeweiligen Aufgaben qualifiziert sein muss, und der Datentreuhänder wäre zumindest im weitesten Sinne eine „beteiligte Person“, wenn er Patientenlisten für die klinische Prüfung verwaltet. Allerdings erfordert die Tätigkeit des Datentreuhänders als solche keine vertieften Kenntnisse im Hinblick etwa auf Durchführung und Ablauf einer klinischen Prüfung oder des einschlägigen Forschungsprojektes, da seine Aufgabe vorrangig darin besteht, die von der Datenbesitzenden Stelle übermittelten personenbezogenen Daten zu anonymisieren bzw. zu pseudonymisieren und sie im Anschluss daran an die Forscher weiterzuleiten sowie diese Daten zu verwalten. In Anbetracht dessen kann auch eine Person ohne Forschungserfahrung qualifiziert für die Aufgabe der Datenverwaltung – auch im Sinne von Art. 2 Abs. 2 der Richtlinie 2005/28/EG – sein, da diese Aufgabe vorrangig Kenntnisse des Datenschutzrechts und nicht praktische Kenntnisse bezüglich medizinischer Forschung erfordert. Es bietet sich allerdings an, dem Datentreuhänder Grundkenntnisse zur Durchführung des jeweiligen medizinischen Forschungsprojektes – etwa in Form eines kurzen Merkblatts o.ä. – zu vermitteln.

Die Regelungen über die Auftragsdatenverarbeitung sind auf die Tätigkeit des Datentreuhänders nicht anwendbar, da eine Weisungsgebundenheit (§ 11 Abs. 3 BDSG) gerade den Sinn des Einsatzes eines Datentreuhänders in Frage stellen würde. Der Datentreuhänder ist auch **nicht** als **verantwortliche Stelle** im Sinne des Datenschutzrechts zu qualifizieren. Denn gemäß § 3 Abs. 7 BDSG ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Dies trifft auf den Datentreuhänder, der an der Verwaltung der Daten gerade kein eigenes Interesse hat, jedoch nicht zu. Dieser befindet sich vielmehr in der Rolle des vertrauenswürdigen Dritten zwischen Datenerhaltender Stelle, dem Betroffenen und dem Forscher[151]. Er ist weder verantwortliche Stelle noch kann seine Tätigkeit der Auftragsdatenverarbeitung zugeordnet werden.

[151] Bizer, DuD 1999, 392, 393

Der Datentreuhänder ist vielmehr „Dritter“ im Sinne von § 3 Abs. 8 S. 2 BDSG, da er ausschließlich als Person bzw. Stelle außerhalb der verantwortlichen Stelle auftritt. Mangels bestehender Weisungsgebundenheit und damit zu verneinender Auftragsdatenverarbeitung gilt für den Datentreuhänder jedenfalls nicht die Vorschrift des § 3 Abs. 8 S. 3 BDSG, wonach von dem Begriff des „Dritten“ Personen und Stellen ausgenommen sind, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen. Auch ist der Datentreuhänder kein „Empfänger“ nach § 3 Abs. 8 S. 1 BDSG, obwohl er im weiteren Sinne durchaus Daten „erhält“. Der Begriff des Empfängers umfasst nämlich lediglich alle Datenempfangenden Organisationseinheiten innerhalb der verantwortlichen Stelle, also z.B. einen Betriebs-/ Personalrat bzw. der verantwortlichen Stelle insoweit zuzurechnenden Auftragsdatenverarbeitern.[152]

Da der Datentreuhänder nicht verantwortliche Stelle im Sinne des Datenschutzgesetzes ist, können die vom Gesetz festgelegten Rechte und Pflichten für diese ebenso wenig als Anknüpfungspunkt dienen wie die Vorschriften über die Auftragsdatenverwaltung. Allerdings lässt sich in § 11 BDSG zumindest ein **Mindeststandard** für den Fall erkennen, dass der Datentreuhänder seinerseits weisungsgebundene Subunternehmer einsetzt. Nach § 11 Abs. 2 BDSG ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftraggeber hat sich zudem von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Es kommt bei der Auftragsdatenverarbeitung darauf an, dass das Auftragsunternehmen einen angemessenen Datensicherungsstandard gewährleisten kann, der den Anforderungen von § 9 BSDG und der Anlage zu dieser Vorschrift entspricht[153]. In der Anlage zu § 9 Satz 1 BDSG (gem. BGBl. I 2003, 88) besteht die Pflicht, insbesondere solche Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

[152] Gola/Schomerus, Kommentar zum BDSG, 7. Aufl., § 3 Rdnr. 51

[153] Simitis, Kommentar zum BDSG, 6. Aufl., § 11 Rn. 43

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Diese Grundsätze bieten eine gewisse Orientierungshilfe für die Auswahl geeigneten Personals, das der Datentreuhänder hinzuzieht. Bei der Auswahl seines Personals sollte der Datentreuhänder die fachliche und persönliche Eignung überprüfen und sich zur Beaufsichtigung der fachlichen Qualität und der Verschwiegenheit seines Personals gegenüber seinem Vertragspartner (bspw. den Beteiligten der klinischen Prüfung, TMF) **vertraglich** verpflichten. Es empfiehlt sich, dass der Datentreuhänder seinerseits **schriftliche Vertraulichkeitsvereinbarungen** mit seinem Hilfspersonal schließt und diese auf Verlangen den betroffenen oder den sonst an der klinischen Prüfung beteiligten Personen vorzeigt.

Ein angemessener Datensicherungsstandard sollte indessen auch von dem Datentreuhänder selbst gefordert werden. Hierfür eignet sich ebenfalls der Abschluss einer entsprechenden privatvertraglichen Vereinbarung mit dem Datentreuhänder, durch welche entsprechende Standards hinsichtlich der Datensicherung festgelegt werden können. Diese Standards sollten sich idealerweise an den Anforderungen des § 11 Abs. 2 und Abs. 3 BDSG orientieren.

Es ist selbstverständlich schließlich auch zu fordern, dass zwischen den Forschern und dem Datentreuhänder (bzw. dessen Personal) eine **personelle und räumliche Trennung** bestehen muss.[154] Eine solche Trennung sollte auch mit allen anderen, die an den Patientendaten ein Interesse haben könnten (insbesondere Sponsoren klinischer Prüfungen, aber auch klinische Prüfeinrichtungen) bestehen. Einen ähnlichen Ansatz verfolgt auch Art. 2 des Bayerischen Krebsregistergesetzes[155] mit der Trennung von Vertrauensstelle und Registerstelle: **„**Das bevölkerungsbezogene Krebsregister Bayern besteht aus einer selbständigen Vertrauensstelle und einer selbständigen Registerstelle, die jeweils räumlich, organisatorisch und personell voneinander getrennt sind und unter ärztlicher Leitung stehen.“

[154] Materialien zum Datenschutz, 6.2, unter www.datenschutz-berlin.de

F2.11 Wo verbleiben die gespeicherten Daten, falls die Finanzierung des Datentreuhänders nicht weiter gewährleistet ist?

Die Gewährleistung der Finanzierung kann einerseits entfallen, wenn der Auftraggeber des Treuhänders diesen nicht mehr weiter finanzieren kann oder will. Wenn die Finanzierung des Datentreuhänders nicht mehr gewährleistet ist, wird dieser grundsätzlich gem. § 320 BGB von seiner Leistungspflicht frei, da bei einem entgeltlichen gegenseitigen Vertrag jeder Teil nur gegen Erbringung der Gegenleistung zur Leistung verpflichtet ist. Allerdings gelten unabhängig von den zivilrechtlichen Vorschriften weiterhin zwingend die Regelungen des öffentlichen Datenschutzrechts. Die Datenschutzgesetze treffen zwar den Auftraggeber bzw. die Datenhaltende Stelle und nicht den Datentreuhänder, der keine verantwortliche Stelle ist. Allerdings besteht ein nachvertragliches Treueverhältnis zwischen dem Datentreuhänder und dem Auftraggeber. Daher muss der Datentreuhänder zumindest eine geordnete Abwicklung des Vertragsverhältnisses gewährleisten sowie seine passiven Sicherungspflichten hinsichtlich der von ihm verwalteten Daten der Betroffenen wahrnehmen.

Die Finanzierungsgewährleistung kann auch dann fehlen, wenn der Datentreuhänder während des laufenden Vertragsverhältnisses insolvent wird.

Die Frage, was bei Beendigung des Datentreuhändervertrages mit den Daten geschieht, sollte vorab unter allen beteiligten Personen und Institutionen **vertraglich** geregelt werden. Folgende Konstellationen sind nach Ausscheiden des Datentreuhänders möglich:

(1) Die Identitätsverwaltung durch einen Datentreuhänder endet und der Reidentifikationsschlüssel verbleibt allenfalls noch in Kenntnis des (behandelnden) Arztes, der das Pseudonym für die betroffene Person ursprünglich angefordert hatte.

(2) Der Reidentifikationsschlüssel wird an einem nachfolgenden Datentreuhänder übertragen, der die Identitätsverwaltung mit den gleichen Anforderungen durchführt wie der ausscheidende Datentreuhänder.

(3) Die Daten der Patienten werden mit Ausscheiden des Datentreuhänders vollständig anonymisiert und nur noch in dieser Form weiter genutzt. In diesem Fall bedarf es keiner treuhänderischen Verwaltung des Reidentifikationsschlüssels durch einen Datentreuhänder oder den Arzt.

Die Möglichkeit, dass alle beteiligten Personen (Sponsoren klinischer Prüfungen, externe Forscher, Prüfärzte, behandelnden Ärzte) nach Ausscheiden des Datentreuhänders einen Reidentifikationsschlüssel der betroffenen Person erhalten, scheidet selbstverständlich aus. Ein

[155] G. v. 25.07.2000, GVBl S. 274, zuletzt geändert durch G. vom 24.12.2005, GVBl. S. 652

solches Vorgehen wäre mit den Erfordernissen der medizinischen Forschung nicht mehr zu rechtfertigen und würde auch dem Sinn und Zweck der Pseudonymisierung zuwiderlaufen.

Aus Sicht der betroffenen Person und auch unter Berücksichtigung der Erfordernisse der medizinischen Forschung dürften nur die Konstellationen (1) und (2) in Frage kommen. Der Fall (3) bietet zwar einen Datenschutz für die betroffene Person, jedoch könnte sie andererseits auch Nachteile erleiden, weil bspw. sich aus der Analyse der Forschungsdaten mögliche neue und bessere Behandlungsoptionen, auch Optionen auf Teilnahme an weiteren Studien ergeben, die der betroffenen Person mangels Identifizierbarkeit nicht mehr mitgeteilt werden können. Zudem hat die medizinische Forschung mit Datensammlungen in der Regel ein anerkennenswertes Interesse an der Rückverfolgbarkeit in gewissen Fällen.[156] Daher würde der Wert der Forschung erheblich geschmälert werden, wenn bei Beendigung des Vertrages mit dem Datentreuhänder die Daten nur noch irreversibel anonymisiert zur Verfügung stünden. Es verbleiben somit die Konstellationen (1) und (2).

Es ist allerdings nicht erforderlich, bereits in der Patienteneinwilligung über die Einbindung des Datentreuhänders über beide Konstellationen zu informieren und dem Patienten eine optionale Einwilligung anzubieten. Ein derartiges Vorgehen, das eine Einwilligung des Betroffenen im

[156] Vgl. Dazu Bundestags-Drucks. 16/5374 betr. Technikfolgenabschätzung bei Biobanken, S. 76: „Bei heutigen medizinischen Datensammlungen in der Forschung liegen die medizinischen Daten in anonymisiertem Zustand irreversibel entkoppelt von den patientenidentifizierenden Daten vor. Aus wissenschaftlicher und medizinischer Sicht ist das Verfahren der Anonymisierung zwar gängige Praxis, jedoch in drei grundlegenden Fällen unbefriedigend: (1) Wenn Forschungsvorgänge und Behandlungsvorgänge parallel laufen, (2) wenn eine langfristige Beobachtung des Patienten mit entsprechend longitudinaler Fortschreibung der Forschungsdaten gewünscht ist und dies mehrzeitige Datenexportvorgänge oder Behandlungsschritte an unterschiedlichen Institutionen erfordert, (3) wenn sich aus einer Analyse der Forschungsdaten (durch nichtbehandelnde Ärzte und Wissenschaftler) mögliche neue und bessere Behandlungsoptionen, auch Optionen auf Teilnahme an weiteren Studien ergeben können, die man dem Patienten mitteilen muss. Für den ersten und zweiten Fall ist die Fortschreibung des „anonymen“ Falls in den Forschungsdatenbanken oder Kohorten (Registern) erforderlich, sodass trotz Auslassung patientenidentifizierender Merkmale die Daten immer derselben Person zugeordnet werden können. Im dritten Fall ist zusätzlich eine Rückermittlung der dahinterstehenden Person anhand eines primär „anonymen“ Falls erforderlich. In diesen Fällen ist eine reine Anonymisierung nicht adäquat, da weder eine Fallfortschreibung noch eine – hier gewollte – Reidentifikation der Person möglich sind. Daher muss bei diesen Anforderungslagen, wie sie bei einer Vielzahl von Forschungsdatenbanken und Registern, aber auch beim Aufbau von elektronischen Patientenakten im Rahmen der „vertikalen Vernetzung“ und integrierten Versorgung gegeben sind, stattdessen mit einer Pseudonymisierung operiert werden.“

Hinblick auf unterschiedliche Optionen eines weiteren Verfahrens nach einer eventuellen späteren Insolvenz des Treuhänders umfasste, würde im Übrigen mit hoher Wahrscheinlichkeit die Mehrzahl der Patienten überfordern. Es ist daher unserer Auffassung nach ausreichend, die Betroffenen im Rahmen der Aufklärung darüber zu informieren, dass eine einer bestimmten Berufsgruppe zugehörige Person – z. B. ein Notar – als Datentreuhänder eingesetzt wird. Der Datentreuhänder muss gerade nicht namentlich benannt werden. In diesem Fall wäre es bei einem eventuellen Wechsel des Datentreuhänders auch nicht erforderlich, neue Einwilligungserklärungen der Patienten einzuholen.

Indessen dürften Zwischenformen, wie etwa dergestalt, dass nach Ausscheiden des Datentreuhänders der behandelnde Arzt zeitweise den Reidentifikationsschlüssel verwaltet, bis ein neuer Datentreuhänder die Aufgabe übernimmt, unzulässig sein. Die Rolle des Datentreuhänders als neutrale und vertrauenswürdige Institution würde wohl in Frage gestellt, wenn seine Pflichten zeitweise mit anderen Personen auf vertikaler Ebene geteilt würden.

F2.12 Welche Auskunftspflichten gelten für einen Datentreuhänder gegenüber dem Auftraggeber und gegenüber Patienten, die in die Patientenliste eingeschlossen sind? Sind diese abhängig von einer Patienteneinverständniserklärung?

2.12.1 Inhalt des Auskunftsanspruchs

Die betroffene Person hat jedenfalls einen Auskunftsanspruch nach § 34 BDSG: Der Betroffene kann danach insbesondere Auskunft verlangen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

Der Betroffene muss aber die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen (§ 34 Abs. 2 BDSG). Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, kann der Betroffene über Herkunft und Empfänger nur Auskunft verlangen, sofern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt. In diesem Fall ist Auskunft über Herkunft und Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind (§ 34 Abs. 2 BDSG).

Die Auskunft wird schriftlich erteilt, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist (§ 34 Abs. 3 BDSG). Die Auskunft darf nur in bestimmten Ausnahmefällen entgeltlich sein (§ 34 Abs. 5 BDSG).

Auskunftsanspruch in medizinischen Datensammlungen bzw. Kompetenznetzen

In medizinischen Datensammlungen bzw. Kompetenznetzen kann es sich gebieten, den betroffenen Personen über § 34 BDSG hinaus einen verstärkten Auskunftsanspruch zu geben. Gerade in vernetzten und pseudonymisierten Systemen kann durch ein Auseinanderfallen von der Stelle, die die Identitätsverwaltung vornimmt und der Stelle, die die pseudonymisierten Inhaltsdatensätze besitzt, der Auskunftsanspruch der betroffenen Person erschwert sein.[157] Zur Lösung des Problems könnte es sich anbieten, der betroffenen Person einen Auskunftsanspruch direkt gegen den Datentreuhänder zu geben (dazu 6.3). Zudem müssen die Besonderheiten bei medizinischen Datensammlungen bzw. Kompetenznetzen beachtet werden. Möglicherweise haben dabei die betroffenen Personen einen Anspruch auf Rückmeldung gewonnener medizinischer bzw. wissenschaftlicher Erkenntnisse. Sollen die Daten aus der klinischen Forschung einem **Kompetenznetz bzw. einer medizinischen Sammlung** zu Forschungszwecken zugeführt werden – in die Nutzung zu diesen Zwecken hat die betroffene Person selbstverständlich vorher einzuwilligen – können sich aus der Analyse der Forschungsdaten **mögliche neue und bessere Behandlungsoptionen**, auch Optionen auf Teilnahme an weiteren klinischen Studien ergeben, die man dem Patienten u. U. mitteilen sollte.[158] Ob den Betroffenen tatsächlich ein Rechtsanspruch auf Rückmeldung im Rahmen klinischer Arzneimittelprüfungen zusteht, kann und muss hier nicht abschließend präjudiziert werden. Eine dahingehende ausdrückliche Anspruchsgrundlage für die Betroffenen existiert jedenfalls nicht. Festzuhalten ist, dass medizinische Datensammlungen und Kompetenznetze keineswegs vorrangig der Realisierung von individuellen Therapieoptimierungsmöglichkeiten zu dienen bestimmt sind bzw. dies auch nicht ihrem Zweck entspricht. Auch das Ausfindigmachen der Betroffenen im Einzelfall wird sich in der Praxis als ein kaum überwindbares Hindernis darstellen. Insofern ist das Bestehen eines Anspruchs der Betroffenen auf Rückmeldung eher abzulehnen. Allenfalls bei lebenswichtigen Informationen kann und wird eine Verpflichtung der Verantwortlichen bestehen, einzelne Betroffene persönlich in Form einer Rückmeldung zu kontaktieren .[159]

Es wäre überdies fraglich, wer in berechtigter Weise eine Rückmeldung erhalten sollte. Die betroffene Person ist möglicherweise nicht mehr in Behandlung bei dem Arzt, der ursprünglich das Pseudonym angefordert hatte. Es kann sich empfehlen, bereits im Rahmen der

[157] Weichert, DuD 2006, 694, 696

[158] siehe Bundestags-Drucks. 16/5374, S. 76; dort als eines der Gründe genannt, die eine pseudo-nymisierte statt eine anonymisierte Nutzung von Daten bei medizinischen Datensammlungen erforderlich machen können.

[159] Vgl. Stellungnahme des Nationalen Ethikrates: Biobanken für die Forschung, 2004, S. 68

Patienteneinwilligung über die Einbindung des Datentreuhänders eine Einwilligung des Patienten einzuholen, ob und in welcher Form bzw. an wen er eine Mitteilung wünscht, wenn sich aufgrund der Forschung mit der Datensammlung bessere Behandlungsoptionen ergeben. Allerdings ist zu bedenken, dass eine frühzeitige Einwilligung des Patienten zu der Frage, wer zu einem späteren Zeitpunkt ggf. Rückmeldungen erhalten soll, kaum praktikabel sein dürfte. Der Betroffene wird dies im Zeitpunkt seiner Einwilligung häufig noch gar nicht wissen können. Zudem sollen medizinische Datensammlungen und Kompetenznetze in der Regel der Allgemeinheit der Erkrankten dienen; demnach ist das zwingende Verfolgen von individuellen Therapieoptimierungsmöglichkeiten oft nicht möglich oder entspricht nicht der Zielsetzung der Datensammlung. Es sollte daher vertraglich (auch in der Patienteneinwilligung) eine etwaige Erwartungshaltung ausgeschlossen werden, dass jeweils der Betreiber der Datensammlung oder der Datentreuhänder ungefragt zur Rückmeldung von neuen medizinischen Erkenntnissen in jedem individuellen Fall verpflichtet sind. Es kann nicht verlangt werden, dass jeder Betroffene – ggf. auch unaufgefordert – über alle Ergebnisse der Forschung informiert werden müsste, da dies in vielen Fällen einen nicht bzw. kaum zu leistenden Aufwand bedeutete. Zum einen kann es erhebliche Probleme bereiten, die Betroffenen wieder aufzufinden; zum anderen müssten den Betroffenen ihre persönlichen Befunde im Rahmen einer medizinischen Beratung eingehend erläutert werden, und sie müssten darüber hinaus auch über die möglichen Konsequenzen hieraus beraten werden.[160] Daher sollte erst auf Auskunftsersuchen der behandelnden Ärzte oder der betroffenen Person hin eine Auskunft über die neuen medizinischen Erkenntnisse erfolgen.[161] Allerdings kann sich, wie bereits dargestellt, bei lebenswichtigen Informationen eine Verpflichtung des Verantwortlichen ergeben, über die normale Kommunikation mit der Fachöffentlichkeit hinaus den persönlichen Kontakt mit den Betroffenen zu suchen.[162] Unabhängig davon sollte vertraglich näher ausgestaltet werden, in welchen Fällen, in welchen Abständen und unter welchen Voraussetzungen solch einem Auskunftsersuchen über die medizinischen und wissenschaftlichen Erkenntnisse nachgekommen werden muss. So lange der Mindeststandard von § 34 BSDG nicht unterschritten wird, ist die Datenspeichernde Stelle nicht verpflichtet, über alle Erkenntnisse der Datensammlung ungefragt Auskunft zu geben, so dass ein gewisser Raum für vertragliche Vereinbarungen gegeben ist.

[160] So zur Interessenlage bei Biobanken Stellungnahme des Nationalen Ethikrates: Biobanken für die Forschung, 2004, S. 68

[161] Vgl. Weichert, DuD 2006, 694, 696

[162] Stellungnahme des Nationalen Ethikrates: Biobanken für die Forschung, 2004, S. 68

2.12.2 Dass medizinische Datensammlungen Besonderheiten aufweisen, zeigen auch etwa einige Krebsregistergesetze. So bestimmt etwa § 10 des Hessischen Krebsregistergesetzes[163]:

> „Auf Antrag einer Patientin oder eines Patienten hat die Vertrauensstelle einer oder einem von diesen benannten Ärztin oder Arzt, Zahnärztin oder Zahnarzt mitzuteilen, ob und welche Eintragungen zur Person gespeichert sind. Die Benannten dürfen die Betroffenen über die Auskunft der Vertrauensstelle nur mündlich oder durch Einsichtgabe in die Mitteilung informieren, sofern diese über ihre Erkrankung unterrichtet sind. Weder die schriftliche Auskunft der Vertrauensstelle noch eine Kopie oder Abschrift davon dürfen an die Erkrankte oder den Erkrankten weitergegeben werden. Auch mit Einwilligung der Betroffenen dürfen die Benannten die ihnen erteilten Auskünfte weder mündlich noch schriftlich an Dritte weitergeben.“

2.12.3 Auskunftsverpflichteter

In elektronischen Sammlungen und Netzen medizinischer Daten besteht die Gefahr, dass die Auskunfts- und Einsichtsrechte der betroffenen Personen geschmälert werden, wenn die Daten nicht mehr lokalisierbar sind bzw. die für die Korrektheit der Daten verantwortliche Stelle nicht mehr bestimmbar ist.[164] Mit Blick darauf spricht vieles dafür, dass bei der beabsichtigten klinischen Prüfung der **Datentreuhänder – ggf. neben weiteren – zum Auskunftsverpflichteten** gegenüber dem Patienten wird.

Ein Auskunftsanspruch allein gegen die anderen Beteiligten wäre für den Patienten unzureichend. Dies zeigt sich bspw. bei klinischen Studien. Der behandelnde Arzt bzw. Prüfarzt, der das Pseudonym für den Patienten angefordert hatte, würde in diesem Fall zwar das Pseudonym des Betroffenen kennen, jedoch ggf. nicht alle Daten, die im Laufe der Zeit in der Datensammlung bzw. dem Kompetenz- bzw. Forschungsnetz über den Betroffenen gespeichert sind. Die anderen Prüfarzte, Forscher und der Sponsor würden wiederum das Pseudonym des Patienten nicht kennen und könnten somit keine Auskunft geben.

Dass eine Vertrauensstelle zum Auskunftsverpflichteten für die betroffene Person wird, entspricht auch der Konzeption von § 4 (5) des Hessisches Krebsregistergesetzes[165]:

> „Die Vertrauensstelle erteilt Auskünfte nach § 10 oder fordert dazu, soweit die Daten in der Vertrauensstelle nicht mehr vorliegen, diese von der Registerstelle an.“

[163] G. v. 17.10.2001 (GVBl. I 2001, 582) i. d. Gültigkeit v. 01.12.2007

[164] Menzel/Schläger, DuD 1999, S. 70 ff (S. 74); Weichert, DuD 2006, 694, 696

[165] G. v. 17.10.2001 (GVBl. I 2001, 582) i. d. Gültigkeit v. 01.12.2007

F2.13 Welche Regelungen sind zur Sicherung einer dauerhaften Verfügbarkeit der Daten für den Auftraggeber zwischen Auftraggeber (TMF bzw. Kompetenznetz/Arzt) und Auftragnehmer (Treuhänder) zu treffen? (Datensicherheit, Backup, Ausfallsicherheit etc.)

Die Datensicherung (bzw. Bestrebungen, den Datenverlust bei einem Systemausfall möglichst gering zu halten), ist ein technischer Vorgang. Aus juristischer Sicht ist es von Bedeutung, eine solche **Pflicht** des Datentreuhänders zur **Datensicherung** explizit in den **Vertrag** aufzunehmen, da ihn nicht bereits die gesetzliche Pflicht zur Datensicherung aus § 9 BDSG trifft. Auf diese Weise kann für den Auftraggeber gewährleistet werden, dass nur derjenige als Datentreuhänder fungiert, der die Sicherheit und Verfügbarkeit selbst oder durch Beauftragte schuldet. Der Datentreuhänder kann sich dann auch nicht etwa darauf berufen, dass ihm nicht zuzumuten sei, selbst die erforderlichen technischen Kenntnisse und die technischen Umsetzungsmöglichkeiten für die ausreichende Sicherung des Datensystems zu haben, das ihm – bspw. von Dritter Seite – zur Verfügung gestellt wurde. Der Datentreuhänder muss technisch selbst oder durch seine Beauftragten für die Datensicherheit sorgen. Eine entsprechende Pflichtenbeschreibung ist in den Datentreuhändervertrag aufzunehmen. Von besonderer Bedeutung ist dabei eine Regelung über die zeitlichen Abstände und technischen Modalitäten der Datensicherungsmaßnahmen. Eine übliche, mindestens jedoch einmal wöchentliche Datensicherung ist vorzunehmen, d.h. Duplikate der versicherten Daten sind anzufertigen und so aufzubewahren, dass sie von einem Schadensfall der Originale voraussichtlich nicht gleichzeitig betroffen sein können Zu regeln wäre auch, welche Sicherungsdatenträger zu benutzen sind. Ebenso von Bedeutung dürfte die Festlegung von spezifischen Maßnahmen zur Abwehr von Viren sein, so bspw. Schreibschutz bei allen Disketten, auf die nicht geschrieben werden muss, Verwendung aktueller Virenschutzsoftware, Überprüfung aller neu erworbenen Programme und Datenträger auf Viren, Erstellung von Notfall-Disketten, Schutz der Computer und Datenträger vor unbefugter Benutzung, Klärung der Verfahrensweise bei Verdacht des Virenbefalls.[166]

Hat der Datentreuhänder dann keine im Sinne des Vertrages ausreichende Sicherung vorgenommen (selbst oder durch seine Beauftragten – Erfüllungsgehilfen nach § 278 BGB –), entstünden Schadensersatzansprüche (§ 280 Abs. 1 BGB). Prinzipiell kann der Schadensersatzanspruch des Auftraggebers in diesem Fall den Ersatz jeder Vermögenseinbuße erfassen, die ohne das schädigende Ereignis (fehlende Errichtung einer Datensicherung) nicht

[166] Vgl. Maßnahmenvorschläge gemäß dem Band „Computerviren“ der Schriftenreihe zur IT-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik (BSI), abgedruckt bei Gola/Schomerus, Kommentar zum BDSG, 7. Aufl. 2002, § 9 Rdnr. 19.

eingetreten wäre, § 249 BGB. Der Schadensersatzanspruch entfällt allerdings, wenn der Datentreuhänder nachweist, dass ihn kein Verschulden trifft (§ 280 Abs. 1 BGB). Möglich wäre es auch, für den Fall der mangelnden Sicherung eine Vertragsstrafe zu vereinbaren.

F2.14 Welche Schadenersatzregelungen sollten für den Fall einer Nichtverfübarkeit der Daten getroffen werden? Wie ist Schadensersatz und Haftung bei z.B. Datenverlust sichergestellt? Ist eine Versicherung möglich?

Für die Nichtverfügbarkeit von Daten würde der Datentreuhänder in zwei Fällen haften, nämlich

1. wenn er eine Garantie für die Verfügbarkeit übernommen hat oder
2. wenn er schuldhaft (d.h. durch ein fahrlässiges oder ein vorsätzliches Verhalten) die Nichtverfügbarkeit verursacht hat.

Ob eine Garantie nach (1) vorliegt, ist eine Frage der Vereinbarung. Der Datentreuhänder müsste bereit sein, für die Verfügbarkeit der Daten völlig unabhängig von einem Verschulden einstehen zu wollen.

Bei der Verschuldenshaftung nach (2) unterscheidet man Eigenverschulden und Fremdverschulden. Für das Eigenverschulden wird stets gehaftet. Für das Fremdverschulden hat der Datentreuhänder einzustehen, wenn er sich sog. Erfüllungsgehilfen (§ 278 BGB) bedient, also Personen, die er zur Erfüllung seiner vertraglichen Pflichten arbeitsteilig hinzugezogen hat.[167] So führt etwa die Verletzung vertraglich festgelegter Pflichten zur Datensicherung, wie sie oben unter 2.13 dargestellt wurden, zu einem solchen Schadensersatzanspruch, falls der Datentreuhänder nicht nachweisen kann, dass ihn kein Verschulden an einer entsprechenden Pflichtverletzung trifft. Außerdem haftet er, wenn von ihm weisungsabhängige Personen (bspw. Arbeitnehmer) einen Schaden verursachen und er nicht nachweisen kann, dass er diese „Verrichtungsgehilfen“ sorgfältig ausgesucht und überwacht hat (§ 831 BGB).

Fälle, in denen die Nichtverfügbarkeit der Daten nicht auf einem Verschulden des Datentreuhänders beruhen und daher trotz ggf. entstehender Schäden bei TMF vom Datentreuhänder nicht ersetzt werden müssen, sind bei technischen Projekten naturgemäß nicht

[167] Man wird aufgrund des besonderen persönlichen Vertrauens, das der Datentreuhänder in Anspruch nimmt, annehmen müssen, dass er die wesentlichen Pflichten *in persona* schuldet (§ 613 BGB). Zu solchen Pflichten gehören die, die seine Vertrauenswürdigkeit besonders betreffen, wie etwa die Entscheidung über eine Reidentifikation. Bei der Datensicherung kann er sich dagegen Erfüllungsgehilfen bedienen.

nur theoretisch denkbar. So können insbesondere unverschuldete Wartungsarbeiten und technische Defekte die Verfügbarkeit der Daten einschränken.[168] Möchte TMF selbst für diese Fälle einen Ersatz, bietet sich die bereits genannte Garantierklärung an, der der Datentreuhänder zustimmen müsste. Ebenso kann der Datentreuhänder vertraglich gegenüber dem Auftraggeber (TMF) dazu verpflichtet werden, einen **Versicherungsvertrag** mit einem entsprechenden Versicherer für den Fall des Datenverlustes abzuschließen.

Eine Versicherung des Verlustrisikos der durch den Datentreuhänder verwalteten Daten ist grundsätzlich möglich. Die vorübergehende Nichtverfügbarkeit der Daten ist hingegen nicht versicherbar. Auch treffen den Datentreuhänder als Versicherungsnehmer umfassende Pflichten zur Sicherung der Daten.

Gemäß § 1 Abs. 2 b) der Allgemeinen Bedingungen für die Elektronik-Versicherung (ABE) sind zwar Daten, soweit nichts anderes vereinbart ist, nur versichert, wenn sie für die Grundfunktion der versicherten Sache notwendig sind (z. B. System-Programmdaten aus Betriebssystemen oder damit gleichzusetzende Daten). Eine derartige Versicherung wäre für die vorliegend betroffenen Daten aber nicht passend, da es zumindest in aller Regel nicht um den Ausfall der System-Programmdaten gehen wird. Vielmehr ist vorliegend die Verfügbarkeit von (einzelnen) Daten aus Datenbanken betroffen. Für diese ist gemäß Klausel 028 der ABE eine sogenannte weitergehende Softwareversicherung in Form der erweiterten Datenträgerversicherung möglich. Nr. 1 der Klausel 028 ABE betrifft den Gegenstand der Versicherung. Nach Nr. 1 a) sind die im Versicherungsvertrag bezeichneten Daten und Programme, z. B. Daten aus Dateien/Datenbanken, Standardprogramme, individuell hergestellte Programme versichert. Es ist also grundsätzlich möglich, die Patientenlisten als Daten, zugehörig zu einer bestimmten Datenbank, zu versichern. Die Listen bzw. die Datenbank, die sie enthält, müssten dann im Rahmen des Versicherungsvertrages genau bezeichnet werden. Denn es ist im Rahmen einer Versicherung nach Klausel 028 ABE grundsätzlich erforderlich, den Gegenstand der Versicherung zu definieren[169]. Dies bedeutet aber nicht, dass etwa die einzelnen Patientennamen genannt werden müssen, vielmehr genügt die Angabe, dass eine bestimmte technisch identifizierbare Datenbank versichert sein soll. Ohnehin werden bei Pauschalversicherungen vielfach alle Daten und Programme versichert, die sich auf DV-Anlagen des Versicherungsnehmers befinden.[170] Daher ist mit dem Datentreuhänder abzustimmen, ob er bereits einen entsprechenden Versicherungsvertrag hinsichtlich von ihm verwalteter Daten

[168] Beck’sches Formularhandbuch E-Commerce, München 2003, A.1. 10.

[169] Tita, in VW 2001, 1696

[170] Vgl. dazu Tita, in VW 2001, 1697

abgeschlossen hat. Ein derartiger Vertrag könnte dann hinsichtlich der zu verwaltenden Patientenlisten entsprechend erweitert bzw. konkretisiert werden.

Gemäß Nr. 1 a) Klausel 028 ABE sind diejenigen **Datenträger** – Datenspeicher für maschinenlesbare Informationen – mitversichert, auf denen die versicherten Daten und Programme gespeichert sind, sofern diese Datenträger ihrer Bestimmung nach auswechselbar sind, z. B. Magnetwechselplatten, Magnetbänder, Disketten. Nicht versichert sind indessen nach Nr. 1 b) Klausel 028 ABE Daten und Programme, zu deren Nutzung der Versicherungsnehmer nicht berechtigt ist, nicht betriebsfertige bzw. nicht lauffähige Programme sowie Daten und Programme, die sich nur im Arbeitsspeicher der Zentraleinheit befinden, und zwar auch dann nicht, wenn sie im Vertrag genannt sind.[171] Dies ist jedenfalls dann unproblematisch, wenn die in den Patientenlisten enthaltenen Daten ausschließlich auf den eigenen Anlagen des Datentreuhänders als Versicherungsnehmer gehalten, verwaltet und bearbeitet werden. Gemäß Nr. 2 a) Klausel 028 ABE besteht Versicherungsschutz innerhalb der im Versicherungsvertrag bezeichneten Betriebsgrundstücke. Nach Nr. 3 a) Klausel 028 ABE soll die im Versicherungsvertrag für die versicherten Daten und Datenträger genannte Versicherungssumme dem Versicherungswert entsprechen. Versicherungswert sind bei Daten und Programmen die Wiederbeschaffungs- und Wiedereingabekosten, bei Datenträgern die Wiederbeschaffungskosten.

Der Versicherer leistet nach Nr. 4 Klausel 028 ABE **Entschädigung**, wenn eine nachteilige Veränderung oder ein Verlust versicherter Daten oder Programme eingetreten ist durch einen gemäß § 2 ABE versicherten Schaden an dem Datenträger, auf dem sie gespeichert waren, oder an der Datenverarbeitungsanlage, durch die sie verarbeitet wurden. Dieser Absatz umfasst zunächst die Risiken der Datenträgerversicherung. Es handelt sich dabei grundsätzlich um eine „Allgefahrendeckung“.[172] Der Versicherer leistet aber auch dann Entschädigung, wenn eine nachteilige Veränderung oder ein Verlust versicherter Daten oder Programme eingetreten ist durch

a) Störung oder Ausfall der DV-Anlage, der Datenfernübertragungseinrichtungen und –leitungen, der Stromversorgung/Stromversorgungsanlage oder der Klimaanlage;
b) Bedienungsfehler;
c) Computerviren;
d) vorsätzliche Programm- oder Datenänderung durch Dritte in schädigender Absicht;
e) Über- oder Unterspannung (einschließlich Blitzeinwirkung);
f) elektrostatische Aufladung, elektromagnetische Störung;

[171] Voit/Knappmann, in Prölss/Martin, Kommentar zum VVG, 27. Aufl., Klausel 028 ABE Nr. 1 Rdnr. 3

[172] Tita, in VW 2001, 1699

und die versicherten Daten oder Programme deshalb rekonstruiert oder wiederbeschafft werden müssen. Beim Auftreten eines Virus ist, unabhängig davon ob bereits Daten verlorengegangen sind oder noch nicht, von einem Schadensereignis auszugehen, wohingegen Würmer und Trojaner im Einzelfall ggf. differenziert zu betrachten sind.[173] Der Versicherer leistet gemäß Nr. 5 Klausel 028 ABE Entschädigung bei nachteiliger Veränderung oder Verlust versicherter Daten oder Programme in Höhe der notwendigen Kosten für die jeweils erforderliche Wiedereingabe und ggf. Wiederbeschaffung. Allerdings ist bei Schäden gemäß Nr. 4 a) bis f) – siehe soeben – die Entschädigungsleistung (nach Abzug des Selbstbehaltes) je nach Versicherungsfall auf 50 Prozent der im Versicherungsvertrag je Position genannten Versicherungssumme begrenzt. Es ist auch zu berücksichtigen, dass im Rahmen der Softwareversicherung nur die Daten und Programme als solche versichert sind. Gerade **nicht mitversichert** ist die Verfügbarkeit der Daten, also das Risiko, dass durch deren Nichtverfügbarkeit Betriebsunterbrechungen eintreten[174]. Insofern kann der Datentreuhänder das Risiko der Nichtverfügbarkeit der Daten nur in dem Maße versichern, als auf diese dauerhaft nicht mehr zugegriffen werden kann. Denn lediglich in diesem Fall steht die Nichtverfügbarkeit einem Datenverlust gleich. Zu beachten ist auch, dass den Versicherungsnehmer stets die **Obliegenheit der Datensicherung** trifft.[175] Die Obliegenheiten des Versicherungsnehmers werden in Nr. 6 Klausel 028 ABE aufgeführt. Der Versicherungsnehmer hat nach Nr. 6 a) eine übliche, mindestens jedoch einmal wöchentliche Datensicherung vorzunehmen, d.h. Duplikate der versicherten Daten anzufertigen und so aufzubewahren, dass sie von einem Schadensfall der Originale voraussichtlich nicht gleichzeitig betroffen sein können. Die Datensicherung durch Anfertigung und sachgerechte Aufbewahrung von Duplikaten auf sogenannten Sicherungsdatenträgern ist seitens der Versicherer geboten, um die Kosten in Grenzen zu halten. Diese Obliegenheit ist daher keine Bagatelle.[176] Datensicherung erfüllt nur dann ihren Zweck, wenn die Rekonstruktion sowohl beim Verlust von Daten als auch der gesamten Rechneranlage mit den darauf lagernden Datenbeständen möglich ist.[177] Die Datensicherung erfordert, dass von allen Arbeitsdateien mehrere Generationen von Datensicherungsbeständen bestehen, wobei eine Kopie weitgehend den aktuellen Datenbestand beinhalten muss.[178]

[173] Tita, in VW 2001, 1702

[174] Tita, in VW 2001, 1782

[175] Tita, in VW 2001, 1782

[176] Voit/Knappmann, in Prölss/Martin, Kommentar zum VVG, 27. Aufl., Klausel 028 ABE Nr. 6 Rdnr. 1

[177] Seitz/Bühler, Die Elektronikversicherung, 1994, S. 31.

[178] Tita, in VW 2001, 1785

Verletzt der Datentreuhänder als Versicherungsnehmer die Obliegenheit der Datensicherung – oder eine andere nach Nr. 6 Klausel 028 ABE bestehende Obliegenheit – so ist der Versicherer nach Maßgabe des § 6 Abs. 1 und Abs. 2 VVG zur Kündigung berechtigt oder auch leistungsfrei. Für TMF bedeutet dies im Schadensfall, dass die Versicherung den eingetretenen Schaden nicht übernimmt. Insofern sollte in den Vertrag zwischen TMF und Datentreuhänder die umfassende Datensicherung ebenfalls als Pflicht aufgenommen werden.[179]

F2.15 Wie ist der Zugriffsschutz auf z.B. Sicherungsbänder durchzuführen?

Die Frage des strafrechtlichen Zugriffsschutzes auf Gegenstände, die sich im Gewahrsam des Datentreuhänders befinden, war bereits Gegenstand von F. 2.1 ff.. Hinsichtlich der Sicherungsbänder dürften sich insoweit keine Besonderheiten ergeben. Diese sind zwar „Gegenstände“ bzw. „Datenträger“, bei denen über eine Einbeziehung in die Freiheit von einer Beschlagnahme gem. § 97 StPO diskutiert werden könnte. Allerdings ergeben sich die gleichen Probleme, wie bereits zur Frage der Beschlagnahmemöglichkeit von Patientenlisten ausgeführt (s.o. F.2.3). Sofern also die Sicherungsbänder Forschungsdaten enthalten, fallen sie voraussichtlich nicht unter den Beschlagnahmeschutz nach § 97 StPO trotz ggf. bestehender ärztlicher oder notarieller Zeugnisverweigerungsberechtigung.

Darüber hinaus kann sich die Frage stellen, ob und inwieweit der Datentreuhänder zivilrechtlich verpflichtet ist, den Zugriffsschutz auf die Sicherungsbänder sicherzustellen. Die Anforderungen für die Prüfung der Datensicherung durch die Sicherungsbänder wurden von der Rechtsprechung wie folgt umschrieben:

> Gegenstand einer Funktionsprüfung einer Datensicherung ist, zu überprüfen, ob das, was gesichert werden soll, auch auf ein Band geschrieben wird und ob das, was sich auf dem Sicherungsband befindet, auch wieder vollständig zurückgelesen werden kann. [180]

Darüber hinaus finden sich in der Anlage zu § 9 BDSG konkrete Regelungen zur Datensicherung. Es ist zu fordern, dass der Datentreuhänder auch hinsichtlich seiner Sicherungsbänder alle Maßnahmen gem. der Anlage zu § 9 BDSG erfüllt (dazu unten 2.17).

[179] Siehe hierzu bereits oben unter 2.13

[180] LG Wuppertal, Zivilkammer, Urt. v. 15.10.2003, Az.: 4 O 70/02.

F2.16 Welche Haftungsregelungen gelten für einen Datentreuhänder?

Der Datentreuhänder haftet nach den allgemeinen Regeln, nach denen ein Dienstleister (§ 611 BGB) haftet. Das bedeutet, dass er mangels anderweitiger vertraglicher Regelungen für jeden Schaden haftet, der durch eine Pflichtverletzung des Datentreuhänders entsteht, und auf Vorsatz oder Fahrlässigkeit (§ 276 BGB) des Datentreuhänders oder seiner Erfüllungsgehilfen beruht (§ 280 Abs. 1 BGB). Solche Pflichtverletzungen können bei allen Funktionen des Datentreuhänders auftreten, bspw. Mängel bei Identitätsverwaltung, Mängel bei Pseudonymisierung oder Verlust eines Reidentifikationsschlüssels. Zudem kann ein Verzug mit einer Leistungspflicht (bspw. Erfüllen eines Auskunfts- oder Auswertungsersuchens, Abgabe eines Forschungsberichtes) Schadensersatzansprüche auslösen (§§ 208 i.V. m. 286 BGB). Wichtig ist jedoch, dass bei demjenigen, der einen Schadensersatzanspruch geltend macht, auch tatsächlich ein nachweisbarer Schaden entstanden ist.

Prinzipiell ist möglich, dass die Haftung des Datentreuhänders vertraglich im Rahmen des gesetzlich Zulässigen modifiziert wird. So kann etwa für Vermögensschäden die Haftung des einen oder aller Vertragspartner auf Vorsatz und grobe Fahrlässigkeit beschränkt werden.

Der Datentreuhänder kann auch gegenüber Personen haftet, mit denen er **keinen Vertrag** geschlossen hat **(Deliktshaftung)**. Voraussetzung wäre hierfür, dass der Datentreuhänder entweder schuldhaft bei den Personen einen Schaden an einem sog. absoluten Rechtsgut i. S. v. § 823 BGB (insbes. Leben, Körper, Gesundheit, Freiheit, Eigentum) zufügen würde. Die Möglichkeit einer Haftung nach § 823 Abs. 2 BGB wegen der Verletzung eines Schutzgesetzes scheidet aus, da der Datentreuhänder als Dritter weder verantwortliche Stelle i. S. v. § 3 Abs. 7 BDSG, noch Empfänger i. S. v. § 3 Abs. 8 S. 1 BDSG ist, noch Auftragsdatenverarbeiter nach § 11 BDSG. Er ist damit nicht direkt Adressat der Datenschutzgesetze, so dass auch die teils umstrittene Frage, ob die Bestimmungen der Datenschutzgesetze als Schutzgesetze i. S. v. § 823 Abs. 2 BGB anerkannt werden können, für ihn unerheblich bleibt.[181]

Kompliziert kann die Haftungssituation bei klinischen Prüfungen werden. Erleidet ein Studienteilnehmer durch die Studie einen Schaden an Leben, Körper oder Gesundheit, müsste prinzipiell die Probandenversicherung des Sponsors die Schäden ersetzen (§ 40 Abs. 1 Nr. 8 i. V.

[181] Die herrschende Meinung qualifiziert aber viele Bestimmungen des BDSG als Schutzgesetze im Sinne von § 823 Abs. 2 BGB; vgl. hierzu etwa Bruns, Informationsansprüche gegen Medien, 1997, S. 37, m.w.N; Gola/Schomerus, Kommentar zum BDSG, 7. Aufl. 2002, § 1 Rdnr. 4; im Ergebnis ebenso Palandt/Sprau, BGB, 66. Aufl. 2007, § 823 Rdnr. 62: OLG Hamm, Urteil vom 4.4.1995, Az.: 9 U 42/95; OLG Frankfurt, MDR 2005, 881,882; AG Berlin-Mitte, DuD 2004, 309-312

m. Abs. 3 AMG). Mit Blick auf den denkbaren Fall, dass solche Schäden tatsächlich auf einem Fehlverhalten des Datentreuhänders beruhen, kann es sich empfehlen, vertraglich für solche Fälle sog. Freistellungsvereinbarungen zu schließen, die es Sponsor erlauben, vom Datentreuhänder Ersatz zu verlangen.

F2.17 Gibt es weitere rechtliche Rahmenbedingungen, welche für den Datentreuhänder relevant sind und hier noch nicht berücksichtigt wurden?

Von besonderer Bedeutung für die Arbeitsweise des Datentreuhänders ist, dass er die nach den Datenschutzgesetzen erforderlichen technischen und organisatorischen Maßnahmen für die Datensicherung trifft. Regelungen zur Datensicherung finden sich in § 9 BDSG i.V.m. seiner Anlage. Da der Datentreuhänder aber nicht selbst die „verantwortliche Stelle“ ist, besteht die Möglichkeit, dass er vertraglich zur Einhaltung der Standards nach der Anlage zu § 9 BDSG verpflichtet wird. Der Datentreuhänder hat zu gewährleisten, dass die personenidentifizierenden Daten nicht unbefugt eingesehen oder genutzt werden können. Gem. der Anlage zu § 9 BDSG umfasst dies insbesondere Maßnahmen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

F2.18 Auflistung von Regeln und Leitlinien für die Datentreuhänderschaft

Folgende Regeln und Leitlinien stellen eine Zusammenfassung der zentralen, wenn auch nicht abschließenden, Aspekte der Datentreuhänderschaft dar:

1. Der Datentreuhänder hat eine Vertrauenswürdigkeit zu gewährleisten. Daher sind Berufsgruppen zu bevorzugen wie die Notare, die durch gesetzliche Bestimmungen zur einem vertrauenserhaltenen Verhalten verpflichtet sind (vgl. § 14 Abs. 3 S. 1 BNotarO).

2. Der Notar ist auch Angehöriger einer Berufsgruppe mit gesetzlichem Zeugnisverweigerungsrecht, was nach Möglichkeit zu gewährleisten ist.[182] Zwar kann ein umfassender Beschlagnahmeschutz auch über einen Notar als Treuhänder gemäß §§ 53 f., 97 StPO, § 203 StGB nicht erreicht werden, allerdings sind Durchsuchung und Beschlagnahme von Datenträgern bei Berufsgeheimnisträgern besonders restriktiven Anforderungen bezüglich ihrer Verhältnismäßigkeit unterworfen. Dies gilt insbesondere unter Berücksichtigung von Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Zudem darf in die beim Notar beschlagnahmten Unterlagen grundsätzlich keine Einsicht für Dritte gewährt werden.

3. Der Datentreuhänder verfügt auch über ausreichend rechtliche, organisatorische und technische Kenntnisse. Für den Bereich der technischen Kenntnisse kann er allerdings auch Beauftragte einschalten. Der Datentreuhänder verfügt möglichst auch hinreichende medizinische Kenntnisse, was nicht bedeutet, dass er den Heilberufen oder der medizinischen Wissenschaft angehören muss. Allerdings muss er die rechtlichen Rahmenbedingungen dieser Bereiche kennen, was er vertraglich gegenüber dem Auftraggeber auch zu gewährleisten hat. Der Auftraggeber hat dem Datentreuhänder aber auch alle notwendigen Informationen bezüglich des Forschungsvorhabens zu erteilen, was etwa durch die Übergabe von Merkblättern (evtl. sogar als Anhänge des Datentreuhändervertrages) geschehen kann.

4. Der Datentreuhänder hat Neutralität zu gewährleisten. Trotz seiner vertraglichen Beziehungen zum Auftraggeber ist er bei seiner Aufgabenerfüllung nicht parteiisch, sondern

[182] Vgl. oben S. 23.

gewährleistet die Rolle des vertrauenswürdigen Dritten zwischen der Datenhaltenden Stelle, den Forschern und den Betroffenen. Dies anerkennt der Auftraggeber bzw. die Datenhaltende Stelle auch an.

5. Der Datentreuhänder sorgt im ausreichenden Maße für die Wahrung der Authentizität der Daten und die Datensicherheit. Entsprechende Pflichten sind ihm vertraglich aufzuerlegen. Sie haben sich an dem Schutzniveau des § 9 BDSG auszurichten, auch wenn die Vorschrift den Datentreuhänder nicht unmittelbar trifft.

F2.19 Inhalte eines Datentreuhändervertrages (zwischen TMF und Daten-treuhänder)

Je nach Interessenlage von TMF und den anderen Beteiligten, ergibt sich folgendes Vertragsgerüst, dessen einzelne Punkte in diesem Gutachten teilweise bereits eingehend behandelt wurden:

1. Vertragschließende
2. Vertragslaufzeit
3. Aufgaben des Datentreuhänders, bspw.
    a. Prüfung der gemeldeten Daten auf Schlüssigkeit und Vollständigkeit zu überprüfen
    b. Abgleichung personenidentifizierender Daten
    c. Beschreibung der Prozedur der Verschlüsselung
    d. Genaue Art der Speicherung, bspw. Übernahme der Identitätsdaten und der epidemiologischen Daten auf getrennte Datenträger
    e. Zwecke der Speicherung
    f. Übermittlungspflichten (an wen? / in welchem Umfang? / Fälle der Reidentifikation von Personen etc.)
    g. Behandlung von Auskunftsersuchen
    h. Behandlung von Recherche- bzw. Auswertungsaufträgen
    i. Erstellen von Berichten (welche Berichte? /wann? /an wen? In welcher Form?)
    j. Umfang der Löschung gemeldeter Daten bei Widerruf der Einwilligung eines Betroffenen
    k. Evtl. spezifizierter Pflichten, bspw. wenn eine Einbindung in eine klinische Studie nach § 40 AMG geplant ist. Hier können sich insbesondere Frage der Kooperation mit den Beteiligen (bzw. Sponsoren, Monitore, etc.) ergeben
4. Fragen der Datensicherung (Art und Zeitpunkt von Back-ups, Wartungen, etc.)
5. Fragen der Datenverfügbarkeit und Haftung (einschließlich Freistellungserklärungen, Fragen des Umfang von zu erbringenden Versicherungsnachweisen, Haftung für die Gehilfen;

Haftungsausschlüsse, bspw. bei höherer Gewalt, evtl. Garantieerklärungen, Vertragsstrafen etc.).

6. Anforderungen an das Personal des Datentreuhänders
7. Allgemeines: Schriftform, Gerichtsstand, etc.