4 Rechtliche und ethische Rahmenbedingungen

4.1 Interesse der Patienten – Nutzen für die Forschung[10]

Medizinischer Fortschritt ist nicht ohne die Erhebung, Verarbeitung und Auswertung medizinischer Daten und Proben zu erreichen. Bei der Zusammenführung solcher Daten und Proben zur langfristigen Nutzung sind zunächst scheinbar widerstreitende Interessen zu berücksichtigen. An erster Stelle steht der wichtigste und ausnahmslos anzunehmende Wunsch jedes Patienten, seine individuelle Gesundheit wiederherzustellen bzw. zu erhalten und hierfür eine optimale Behandlung zu bekommen. An zweiter Stelle – in Einzelfällen bereits dem ersten entgegenstehend – steht der ebenso anzunehmende Wunsch jedes Patienten, so wenig wie möglich durch den Heilungs- und Behandlungsprozess beeinträchtigt zu werden. Das oberste Ziel der Forschung, bessere Behandlungsmöglichkeiten zu finden, ist somit zu den Wünschen der Patienten zumeist komplementär. Auf dem Weg dahin benötigen Forscher Behandlungsdaten und biologische Proben von Patienten, um daraus epidemiologische Informationen zu generieren, neue Behandlungsmethoden zu bewerten oder Analyseergebnisse von biologischen Proben mit den Verlaufsdaten der Erkrankungen zu korrelieren. Im Ergebnis kann häufig die Behand-

10 Dieses Kapitel stellt eine Überarbeitung des Kapitels „1 Problemstellung" des einführenden Abschnitts der ersten Version des generischen Datenschutzkonzepts dar [1, S. 2f.]. Einzelne übernommene Formulierungen wurden der Lesbarkeit halber nicht separat gekennzeichnet.

lung künftiger Patienten verbessert und im besten Fall sogar ein unmittelbarer Vorteil an individuelle Studienteilnehmer zurückgegeben werden.

Alle diese Wünsche, Ziele und Möglichkeiten führen dazu, dass der Datenschutz in der medizinischen Forschung eine herausragende Bedeutung hat und haben muss. Es ist im gemeinsamen Interesse von Patienten, behandelnden Ärzten und Wissenschaftlern, alle Gefährdungen oder Beeinträchtigungen der Patienten, die mit der Einwilligung, Diagnostik und Behandlung im Rahmen eines Forschungsverbunds für die Medizin verknüpft sind, so gering wie möglich zu halten. Zu diesem „Gefährdungspotenzial" gehört natürlich auch der ungeeignete Umgang mit personenbezogenen Daten: Selbst ein unfreiwilliger, potenzieller oder latenter Bruch der ärztlichen Schweigepflicht bzw. die Missachtung von Datenschutzbestimmungen in diesem Zusammenhang kann das Verhältnis zwischen Patient und Arzt stören und den Bruch des Vertrauensverhältnisses zwischen Patient und Forschungsverbund zur Folge haben. Als Resultat wären Patienten nicht mehr bereit, dem Forschungsverbund ihr Vertrauen in Form ihrer Mitarbeit zu gewähren, und den Forschungsprojekten wäre ihre Existenzgrundlage und Daseinsberechtigung entzogen.

Die Forschungsverbünde sind daher aus eigenem Interesse an einer alle Mitglieder umfassenden, praktikablen, transparenten und kontrollierbaren Lösung interessiert, die hilft, die Datenschutzbelange ihrer Patienten nachhaltig zu wahren.

4.2 Datenschutzrechtliche Grundlagen

4.2.1 Informationelle Selbstbestimmung

Medizinische Forschung muss immer einen Ausgleich zwischen dem Interesse der Allgemeinheit an medizinischem Fortschritt und den Individualinteressen der beteiligten Probanden hinsichtlich der informationellen Selbstbestimmung anstreben. Die für die Forschung notwendigen Daten werden regelmäßig als besondere personenbezogene Daten gemäß § 3 Abs. 9 BDSG (Gesundheitsdaten) anzusehen sein. Die für diese Datenkategorie speziell formulierten Forschungsklauseln in § 13 Abs. 2 und § 28 Abs. 6 BDSG normieren für den Regelfall einen Vorrang der Verwendung anonymisierter und pseudonymisierter Daten und der Einholung einer Einwilligung. Nur wenn der Forschungszweck auf diesen Wegen nicht oder nur mit einem unverhältnismäßigen Aufwand erreicht werden kann, kann eine gesetzliche Verwendungserlaubnis nach § 13 Abs. 2 Nr. 6 und § 28 Abs. 6 Nr. 4 BDSG greifen [11].

Wenn klinische Daten für ein Forschungsprojekt erhoben werden, ist im Regelfall die Aufklärung der Patienten und das Einholen einer Einwilligung möglich. Anders sieht es hingegen aus, wenn die Daten bereits zu einem früheren Zeitpunkt im Rahmen der Behandlung der Patienten erhoben wurden und

jetzt für die Forschung nutzbar gemacht werden sollen. Einige Landeskrankenhausgesetze (LKG) erlauben die Nutzung und Verarbeitung solcher Daten innerhalb der behandelnden Einrichtung auch zum Zwecke der Forschung (z.B. Art. 27 [4] BayKrG). Allerdings ist zu beachten, dass sich auch zusätzliche Anforderungen durch landesspezifische Gesetze ergeben können, so z.B. eine lokale Pseudonymisierung in Verbundforschungsprojekten (vgl. § 25 [3] LKG Berlin). Sollen die Daten aber zum Zwecke der Forschung weitergegeben werden, bieten selbst weitgehende Regelungen in den Landeskrankenhausgesetzen üblicherweise keine gesetzliche Grundlage. Hier können die speziellen Forschungsklauseln der Datenschutzgesetze greifen, wenn die Übermittlung der Daten zur Durchführung wissenschaftlicher Forschung erforderlich ist, das öffentliche Interesse an dem Forschungsvorhaben das Interesse des Betroffenen an dem Ausschluss einer nicht vereinbarten Nutzung seiner Daten erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit einem unverhältnismäßigen Aufwand zu erreichen ist. Hierzu ist allerdings konkret zu begründen, warum das Forschungsvorhaben nicht mit anonymen oder pseudonymen Daten umgesetzt werden kann und die Einholung der Einwilligung der betroffenen Patienten unzumutbar ist. Zusätzlich kann ein Genehmigungsvorbehalt vorgesehen sein (z.B. § 33 HDSG). Die Höhe der hierfür gesetzlich vorgeschriebenen Hürden reflektiert zudem die Auflagen der ärztlichen Schweigepflicht nach § 203 Abs. 1 StGB.

Die von der TMF beauftragten Rechtsgutachter Roßnagel, Hornung und Jandt formulieren dies zusammenfassend so: „Die forschungsspezifischen Datenschutzregelungen lösen somit den regelmäßig bestehenden Konflikt zwischen den konkurrierenden Grundrechten der Forschungsfreiheit gemäß Art. 5 Abs. 3 GG der Daten verarbeitenden Forschungsstellen und dem Recht auf informationelle Selbstbestimmung der Probanden gemäß Art. 2 Abs. 1 und Art. 1 Abs. 1 GG, indem sie über die Einwilligungsmöglichkeit und die strenge Zweckbindung zu einem interessensgerechten Ausgleich der Grundrechte führen.“ [11, S. C11]

Einen Sonderfall stellt die Mitnutzung von Daten für die Forschung dar, die zu einem anderen Zweck, z.B. dem der Behandlung oder Abrechnung einer Behandlung, erhoben wurden. Das Bundessozialgericht (BSG) kommt in seinem Urteil vom 10.12.2008 zur Weitergabe von Patientendaten durch Leistungserbringer an private Abrechnungsstellen zu dem Schluss, dass die datenschutzrechtlichen Regelungen im SGB so umfassend und detailliert ausgeführt sind, dass eine nachgeordnete Anwendung des Datenschutzrechts nicht mehr im Sinne des Gesetzgebers sein könne [12]. Dementsprechend wären die im SGB aufgeführten Daten und insbesondere die Sozialdaten bei den Leistungserbringern gemäß § 284ff SGB V auch bei Vorliegen einer schriftlichen Einwilligung nicht anders zu verwenden, als dies im SGB konkret vorgesehen ist. Bei dieser Auslegung stützt sich das BSG wesentlich auf den Umstand, dass der Gesetzgeber an anderer Stelle die Zulässigkeit einer auf eine Einwilligung gestützten Datenübermittlung durch Leistungserbringer ausdrücklich geregelt

hat, so z.B. für den Datenaustausch zwischen Hausarzt und anderen Leistungserbringern (§ 73 Abs. 1b Satz 1 und 2 SGB V) [12, Abs. 35]. Dass der Gesetzgeber in § 291a (8) SGB V für ganz bestimmte Datenverwendungen eine Einwilligung explizit ausgeschlossen hat (vgl. Kap. 4.3.2), wird in dem Urteil hingegen nicht gewürdigt. Dieser explizite Ausschluss einer Einwilligung als Rechtsgrundlage würde eher die Schlussfolgerung nahe legen, dass der Gesetzgeber grundsätzlich von der Möglichkeit einer Einwilligungsregelung ausgeht.

In ihrem Rechtsgutachten zur Mitnutzung von Versorgungsdaten in der Forschung kommen Roßnagel und Mitarbeiter zu dem Schluss, dass die Abgeschlossenheit der Regelungen zum Datenschutz im SGB vom BSG nur für die §§ 284ff SGB V schlüssig dargelegt ist. Somit wäre auch nur für diesen Ausschnitt des SGB der Ausschluss einer Einwilligung als Rechtsgrundlage für die Nutzung in der Forschung anzunehmen [11, S. C7]. Zudem weisen die Gutachter darauf hin, dass aus datenschutzrechtlicher Perspektive zwei Kategorien von Daten zu unterscheiden sind: Zum einen gibt es Daten, die für Zwecke der Versorgung erhoben und dokumentiert werden und für die die Regelungen des ärztlichen Berufsrechts und ergänzend des Datenschutzrechts gelten. Davon zu unterscheiden sind die Leistungsdaten als krankenversicherungsrechtliche Sozialdaten, die der Abrechnung von Leistungen der Leistungserbringer im weitesten Sinne dienen. Nur für den Umgang mit letzteren, so die Gutachter, könnten die abschließenden Regelungen des Zehnten Kapitels des SGB V herangezogen werden. Für die Versorgungsdaten seien die Regelungen der § 284ff. SGB V nicht anwendbar, auch wenn ein Datum, wie z.B. die in § 301 Abs. 1 Satz 1 Nr. 3 SGB V genannte Diagnose, inhaltlich in diesen Regelungen erwähnt ist. Eine abschließende Regelung für den Umgang mit Diagnoseinformationen im SGB würde deren Verwendung zu medizinischen Zwecken zu sehr einschränken und sei daher nicht vom Gesetzgeber intendiert [11, S. C8]. Somit bleibt aus Sicht der Gutachter eine Verwendung von Versorgungsdaten auf Basis einer Einwilligung grundsätzlich möglich, vorausgesetzt dass die Daten primär zum Zwecke der Versorgung erhoben wurden und allenfalls sekundär auch für die Abrechnung von Leistungen verwendet werden.

4.2.2 Grenzen von Einwilligungsszenarien

Die rechtlich zulässige Verwendung medizinischer Daten, die die informationelle Selbstbestimmung der Patienten wahren muss, setzt, von wenigen Ausnahmen abgesehen, das Vorliegen einer Einwilligungserklärung voraus. Diese muss freiwillig und ohne Sorge um mögliche Nachteile im Falle einer Verweigerung gegeben werden. Bei der Gestaltung des Aufklärungs- und Einwilligungsprozesses ist zu berücksichtigen, dass sich Patienten aufgrund ihrer Erkrankung von dem behandelnden Personal abhängig fühlen können, das sie um eine Einwilligung bittet. Entsprechend sollte das Gespräch bewusst ergebnisoffen geführt werden. Jede Vermittlung einer Erwartungshaltung in Bezug auf die Antwort des Patienten ist sorgfältig zu vermeiden.

Die Erklärung der Einwilligung muss bestimmt sein, so dass klar zu erkennen ist, unter welchen Bedingungen sich die betroffene Person mit der Erhebung, Verarbeitung oder Nutzung welcher Daten einverstanden erklärt. Aus diesem Grund sind weder Blankoeinwilligungen noch pauschal gehaltene Erklärungen, die den Betroffenen die Möglichkeit nehmen, die Tragweite ihres Einverständnisses zu überblicken, ausreichend. Die Anforderungen an die Bestimmtheit sind umso höher, je größer die Tragweite für die Rechte und Freiheiten der betroffenen Person sind. Gemäß § 4a Abs. 3 BDSG bestehen erhöhte Anforderungen an die Bestimmtheit, wenn sich die Verwendung auf besondere Daten im Sinne des § 3 Abs. 9 BDSG bezieht. Dies schließt explizit Gesundheitsdaten ein. Somit muss für die Einwilligenden klar erkennbar sein, welche Daten, in welcher Form, von wem, wie lange und wofür verarbeitet oder genutzt werden.

Je konkreter die Einwilligung formuliert ist, desto einschränkender und unter Umständen auch problematischer ist sie für die Forschung, und dies gleich in mehrfacher Hinsicht: Je konkreter der Zweck angegeben wird, desto präziser kann auch der notwendige Datensatz, der für die Verarbeitung erforderliche Personenkreis und die hierfür benötigte Projektlaufzeit bestimmt werden. Im Umkehrschluss geht eine zweckoffenere Erhebung und Speicherung im Regelfall auch mit einer geringeren Einschränkbarkeit des Datenumfangs, einer längeren Vorhaltung der Daten und einem größeren mit ihrer Verarbeitung betrauten Personenkreis einher. Dabei ist es sogar häufig auch im Interesse schwer erkrankter Patienten, dass ihre Daten nicht nur einem Forscher mit seinen Spezialinteressen zur Verfügung stehen, sondern von möglichst vielen Experten zur Verbesserung der Behandlungschancen genutzt werden.

Dass es in der medizinischen Forschung oft schwer ist, sich auf eine konkret benennbare Fragestellung zu beschränken, ist weithin anerkannt [13]. Häufig wird daher auch akzeptiert, wenn lediglich krankheitsbezogene Einschränkungen gemacht werden. Ausnahmen hierzu stellen klinische Prüfungen zu Arzneimitteln oder Medizinprodukten dar, die aufgrund der regulatorischen Vorgaben und des geforderten Qualitätsniveaus auf eine Festlegung der Auswertung vor der Datenerhebung angewiesen sind. Aber auch hier kann eine längerfristige Speicherung der wertvollen Daten für zusätzliche Fragestellungen, z.B. zur Generierung neuer Hypothesen, sinnvoll sein. Die Konkretheit der Zweckbezogenheit dient letztlich nur so lange ihrem Ziel der informationellen Selbstbestimmung, wie die Einschränkungen der Forschungsfragestellung von der Mehrheit der Patienten auch nachvollzogen und verstanden werden können. Somit kann auch das Gebot der Verständlichkeit der Einwilligungserklärung schon eine Aufweichung des Prinzips der möglichst engen Definition der Zweckbezogenheit bedeuten. Eine Einschränkung der Forschung auf eine konkrete Unterform der Leukämie wird einem Patienten kaum einen Informationsgewinn bescheren, wenn er diese Unterform nicht ausreichend genau von dem Oberkonzept „Leukämie“ unterscheiden kann.

Jedem Patienten ist hingegen die Unterscheidung zwischen einer zeitlich unbeschränkten Speicherung und einer auf fünf Jahre beschränkten unmittelbar möglich. Ebenso können Patienten zwischen einer Nutzung der Daten nur an einem Klinikum oder auf nationaler oder gar europäischer Ebene unterscheiden. Die mit einer zeitlich unbeschränkten Speicherung einhergehenden Risiken sind jedoch u.U. schwer einschätzbar.

Während eine in Grenzen zweckoffene Erhebung, Speicherung und Verarbeitung medizinischer Daten dem Prinzip einer informierten Einwilligung häufig nicht direkt entgegensteht, verdienen die damit regelmäßig verbundenen Verschiebungen der organisatorischen Rahmenbedingungen eine gesonderte Betrachtung. Die klare Unterscheidbarkeit unterschiedlicher organisatorischer Vorgaben in den Augen der Patienten, wie z.B. der Zeitdauer der Speicherung, empfiehlt diese für die Berücksichtigung in einer abgestuften Einwilligungserklärung [5, S. 97][11]. Auch die Methodik der abgestuften Einwilligungserklärung führt jedoch nicht automatisch zu einer ausreichenden Wahrnehmung bzw. einem informierten Verständnis aller Risiken durch die Patienten.

Mit der verstärkt wahrgenommenen Bedeutung der Biobank-gestützten Forschung in den letzten Jahren ist die Diskussion um eine mögliche Lockerung der Zweckbezogenheit der Einwilligung unter dem Stichwort „broad consent" erneut und kontrovers geführt worden. Der Deutsche Ethikrat hat in einer Empfehlung zu Humanbiobanken für die Forschung gar gesetzlich geregelte Rahmenbedingungen, wie z.B. ein Biobankgeheimnis, gefordert, welches zusammen mit anderen Regelungen eine zweckoffene Einwilligung ermöglichen sollte [15]. Da bisher jedoch völlig offen ist, ob und in welcher Form der Gesetzgeber diesen Vorschlag aufnimmt, bleibt in jedem Einzelfall zu prüfen und abzuwägen, ob der Grad der Bestimmtheit einer Einwilligung den Forschungsinteressen und der Informiertheit der Probanden noch gerecht wird. Risiken, die durch eine längerfristige, vergleichsweise zweckoffene und breit nutzbare Speicherung medizinischer Daten entstehen, sind, wie in dem vorliegenden Leitfaden dargestellt, durch entsprechende technische und organisatorische Maßnahmen und eine langfristig klar geregelte Verantwortlichkeit auszubalancieren (vgl. Kap. 6.7). Der Arbeitskreis Medizinischer Ethik-Kommissionen in Deutschland (AK EK) hat für Biobanken entsprechende Mustertexte zur Aufklärung und Einwilligung veröffentlicht.[12]

Grundsätzlich ist zu beachten, dass eine allgemein formulierte Zweckbestimmung und die entsprechende Einwilligung in eine offenere spätere Nutzung von Proben und Daten immer nur dann eine ausreichende Rechtsgrundlage

11 Der Nationale Ethikrat hat in der Stellungnahme „Biobanken für die Forschung" die abgestufte Einwilligung sogar für verzichtbar erklärt, das Fehlen von Wahlmöglichkeiten verletze nicht das Selbstbestimmungsrecht [14, S. 15].

12 siehe http://www.ak-med-ethik-komm.de/formulare.html

für die Forschung bieten können, wenn die Einholung späterer zusätzlicher Einwilligungen aus technischen oder organisatorischen Gründen nicht machbar ist. In bestimmten Fällen kann für die Rekontaktierung beispielsweise ein Abgleich der Daten mit Melderegistern notwendig sein. Hier ist zu prüfen, ob dies im konkreten Fall rechtlich möglich ist (vgl. Kap. 4.3.4). Wenn später eine zusätzliche Einwilligung eingeholt werden soll, muss auch für diese Rekontaktierung eine Einwilligung der Probanden vorliegen. Bei der Prüfung der Durchführbarkeit einer solchen weiterführenden Einwilligung ist zudem zu klären, ob diese zu einer zu großen Selektions-Verzerrung (selection bias) führen könnte.

4.2.3 Verantwortlichkeiten

Die Speicherung und Verarbeitung sensibler medizinischer Daten und Proben setzt eine juristisch belastbare und für jeden Patienten nachvollziehbare Regelung der Verantwortlichkeit voraus (s. Kap. 6.6). Bei der Planung einer langfristigen und einrichtungsübergreifenden Datensammlung ist von vornherein auch zu überlegen, welche verlässliche und vertrauenswürdige Institution mit ebenfalls langfristiger Perspektive die Verantwortung im juristischen Sinne übernehmen kann. Dies kann ein von einem Forschungsnetz gegründeter Verein sein, es sind aber auch andere Lösungen und Formen denkbar, die als juristische Person ansprechbar sind. Bei der Initiierung einer Datensammlung aus einem geförderten Forschungsprojekt heraus ist auch an Regelungen nach Auslaufen der Förderung zu denken. In jedem Fall sollte eine mögliche Rechtsnachfolge für die zunächst verantwortliche Institution geprüft werden. Die notwendige Transparenz gegenüber den Probanden erfordert die verständliche Darlegung der Verantwortlichkeiten in der Einwilligungserklärung.

Der verantwortlichen Institution, z.B. dem Forschungsnetz e.V., wird empfohlen, ein Gremium zu schaffen, welches für datenschutzrechtliche Fragen und Entscheidungen zuständig ist (s. Kap. 6.6). Bei der Besetzung dieses „Ausschusses Datenschutz" ist darauf zu achten, dass Interessenskonflikte soweit möglich vermieden werden. Das Gremium sollte neben der Beratung einzelner Entscheidungen, z.B. welcher Anfrage nach Daten stattgegeben wird, auch für die Ausarbeitung und Fortschreibung der datenschutzrechtlich relevanten Regelwerke und Policies verantwortlich sein. Das Aufgabengebiet des Ausschuss Datenschutz kann z.T. überlappend mit jenem eines betrieblichen oder behördlichen Datenschutzbeauftragten der beteiligten Einrichtungen oder auch eines Forschungsverbunds als juristischer Person sein. Wenn der Forschungsverbund über einen eigenen Datenschutzbeauftragten verfügt, sollte dieser entsprechend auch Mitglied des Ausschuss Datenschutz werden. In Bezug auf die langfristige pseudonymisierte Aufbewahrung von Gesundheitsdaten kommt dem Ausschuss Datenschutz jedoch eine besondere Verantwortlichkeit zu, die im Regelfall eine Besetzung mit mehreren Personen mit ausreichender Sachkenntnis empfehlenswert erscheinen lässt. Somit sollten auch

alle relevanten Entscheidungen mindestens nach dem Vier-Augen-Prinzip getroffen werden.

4.2.4 Anonymisierung und Pseudonymisierung

Das Bundesdatenschutzgesetz definiert in § 3 Abs. 6 BDSG den Vorgang des Anonymisierens und in § 3 Abs. 6a des Pseudonymisierens. Beide Verfahren werden eingesetzt, um die Zuordnung von Daten zu einer bestimmten oder bestimmbaren Person auszuschließen oder zumindest wesentlich zu erschweren. Somit sind beide Verfahren grundsätzlich geeignet, den Schutzbedarf medizinischer Daten abzusenken, bzw. Risiken, die sich aus der Speicherung und Verarbeitung der Daten ergeben, zu minimieren.

Daten sind nach § 3 Abs. 6 BDSG anonymisiert, wenn sie entweder „nicht mehr" oder „nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können". Während die erste Option als absolute Anonymisierung bezeichnet wird, ist die letztere realistischerweise die häufigere und wird mit dem Begriff der faktischen Anonymisierung belegt [16]. Grundsätzlich wird von einer Anonymisierung ausgegangen, wenn identifizierende und medizinische Daten getrennt werden, keine Zuordnungsregel mehr existiert und anhand der medizinischen Daten allein keine Reidentifizierung möglich ist. Anonymisierte Daten gelten damit für nicht mehr personenbeziehbar, so dass für sie auch das Datenschutzrecht samt Einwilligungsvorbehalt nicht mehr anzuwenden ist [11, S. C35]. Problematisch im Umgang mit anonymisierten Daten ist, dass sich der Status der Anonymität im Laufe der Zeit ändern kann, z.B. wenn ein Nutzer der Daten aufgrund einer bestimmten Kombination medizinischer und sozialer Daten auf die Identität des zugehörigen Patienten schließen kann. In diesem Falle würde es sich wieder um personenbezogene Daten handeln, die entsprechend der Vorschriften der Datenschutzgesetze des Bundes und der Länder zu behandeln wären. Problematisch an einem solchen Szenario ist, dass sich im Vorfeld nicht immer ausreichend präzise einschätzen lässt, ob und wann ein solcher Fall eintreten kann. Zur Vorbeugung wird daher empfohlen, auch anonymisierte Datenexporte nur zweckbezogen an definierte Nutzerkreise abzugeben und insbesondere auf die freie Verfügbarmachung medizinischer Daten im Internet in so genannten Public-Use-Files zu verzichten.

Nach § 3 Abs. 6a BDSG ist Pseudonymisieren das „Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren." Im Unterschied zu anonymisierten Daten besteht bei pseudonymisierten Daten noch eine Zuordnungsregel zu den Identitätsdaten der betroffenen Personen. Die Zuordnungsregel ist jedoch nicht allen Nutzern der Daten bekannt, da sonst der Zweck der Pseudonymisierung nicht erreicht würde. Somit muss

hinsichtlich der Datenschutzanforderungen unterschieden werden zwischen Nutzerkreisen, die die Zuordnungsregel kennen und solchen, die sie nicht kennen. Für die erste Gruppe handelt es sich offensichtlich um personenbezogene Daten gemäß dem Datenschutzrecht. In Bezug auf die Einordnung der Daten für die zweite Nutzergruppe gibt es jedoch unterschiedliche Auffassungen. Roßnagel kommt in einem für die TMF erstellten Rechtsgutachten zu dem Schluss, dass pseudonymisierte Daten für Nutzer ohne Zugriff auf die Zuordnungsregel anonymisierten Daten gleichgestellt werden können, wenn „nach der allgemeinen Lebenserfahrung oder dem Stand der Wissenschaft die Zuordnung der Daten zu einer Person praktisch ausscheidet" [11, S. C33]. Eine andere Position wird von Bizer vertreten, der die Möglichkeit einer „relativen Anonymisierung" für Nutzer ohne Zugriff auf die Zuordnungsregel grundsätzlich verneint [17, RN 217; 18]. Auch Roßnagel weist aber darauf hin, dass pseudonymisierte Daten z.B. prinzipiell nicht in Public-Use-Files veröffentlicht werden sollten, da es dann immer Nutzer gibt, die die Zuordnungsregel kennen und damit das Prinzip der Informationsaufteilung umgehen können [11, S. 36]. Zudem bedeutet das Vorhandensein einer Zuordnungsregel auch, dass ein Datensatz hinsichtlich seines inhärenten Reidentifizierungspotenzials nicht abschließend beurteilt werden kann, da grundsätzlich weitere Daten, z.B. aus Follow-ups, zugeordnet werden können. Im Ergebnis empfiehlt auch Roßnagel, den Umgang mit pseudonymisierten Daten am Datenschutzrecht auszurichten, da die Gefahr einer Reidentifizierung zumeist nicht ausreichend sicher ausgeschlossen werden kann.

Ein Sonderfall der Pseudonymisierung besteht dann, wenn eine kryptographische Einwegfunktion zur Generierung der Pseudonyme verwendet wird. In diesem Fall ist kein Schlüssel zur Umkehrung der Pseudonymisierung vorhanden, oder dieser kann bei Nutzung eines asymmetrischen Verschlüsselungsverfahrens vernichtet werden. Somit erlaubt auch die Kenntnis der Zuordnungsregel keine direkte Zuordnung des Pseudonyms zu den identifizierenden Daten. Hierfür hat sich auch der Begriff „Einwegverschlüsselung" etabliert. Es stellt sich dabei die Frage, ob Daten mit nur noch unidirektional vorhandener Zuordnungsregel anders zu bewerten sind, als medizinische und identifizierende Daten, bei denen eine Zuordnung zumindest von einer bestimmten Benutzergruppe in beide Richtungen vorgenommen werden kann. Grundsätzlich wird bei solchen asymmetrischen Verfahren empfohlen, diese so ausprobiersicher zu machen, dass bis auf einen definierten Nutzerkreis niemand Probeverschlüsselungen mit beliebigen identifizierenden Daten machen kann. Dies bedeutet, dass mindestens einer der verwendeten Schlüssel geheim gehalten wird und der Zugang zu dieser Funktion nur autorisierten Nutzern gewährt wird. Trotzdem wird mindestens eine Nutzergruppe weiter Zugang zu dem Verfahren haben und entweder Probeverschlüsselungen vornehmen oder sogar identifizierende Daten als Nutzdaten an dem Verschlüsselungsverfahren „vorbei" schicken können, so dass auf der anderen Seite des Verfahrens identifizierende Daten mit dem asymmetrisch generierten Pseu-

donym im Zusammenhang auftauchen. Abgesehen von solchen Risiken werden aber auch solche asymmetrischen Verfahren hauptsächlich dann eingesetzt, wenn den einmal pseudonymisierten Daten später noch weitere Daten zugeordnet werden sollen. Damit fallen solche Daten auch bezüglich der Problematik des nicht abschließend zu beurteilenden inhärenten Reidentifizierungsrisikos in die gleiche Kategorie, wie die zuvor beschriebenen pseudonymisierten Daten. Entsprechend kommt auch Roßnagel in seinem Gutachten [11, S. C39] zu dem Schluss: „Solange die Identitätsdaten zu den verschlüsselten Behandlungsdaten noch vorhanden sind, besteht grundsätzlich ein höheres Risiko der Reidentifizierung, als wenn die Identitätsdaten vernichtet worden wären. Besteht darüber hinaus eine Zuordnungsregel, sind die Daten pseudonymisiert und nicht anonymisiert." Demzufolge sind pseudonymisierte Daten unabhängig von der Verwendung einer Einwegfunktion zur Generierung des Pseudonyms von ihrem rechtlichen Status her zwischen den personenbezogenen und den anonymen Daten einzuordnen.

Einwegfunktionen ermöglichen die Generierung des immer gleichen Pseudonyms bei identischen Ausgangsdaten. Dies ermöglicht die Erstellung von Pseudonymen auf Basis der identifizierenden Daten von Patienten und erlaubt somit gleichzeitig, auf eine zentrale und langfristige Speicherung der identifizierenden Daten zu verzichten. Somit entfällt die Notwendigkeit, die identifizierenden Daten langfristig und z.B. mit Hilfe eines Treuhänders zu schützen. Auf der anderen Seite entfällt in einem solchen Szenario regelmäßig die Möglichkeit, die beteiligten Patienten zu einem späteren Zeitpunkt sicher zu kontaktieren. Ein weiterer und weniger offensichtlicher Nachteil ist die eingeschränkte langfristige Sicherheit des Pseudonyms. Dessen Sicherheit fußt auf der kryptographisch gesicherten Unumkehrbarkeit des verwendeten Algorithmus, die jedoch nach aller Erfahrung nicht dauerhaft gegeben sein wird.

Die vergleichende Betrachtung der beiden Verfahren der Anonymisierung und Pseudonymisierung zeigt, dass sich der Sicherheitsvorteil der Anonymisierung aufgrund der heute häufig benötigten umfangreichen medizinischen Datensätze mit ihrem inhärenten Reidentifizierungsrisiko stark relativiert. Bei der Wahl des passenden Verfahrens zur Absenkung des Schutzbedarfs medizinischer Daten ist aber noch entscheidender, dass viele Anwendungsfälle mit anonymisierten Daten nicht umgesetzt werden können. Neben der Notwendigkeit, klinische Daten mit Hilfe von Follow-ups im langfristigen Verlauf studieren zu können, ist hier auch die Möglichkeit des individuellen Feedbacks z.B. über neue Therapiemöglichkeiten, Risiken oder Zufallsbefunde zu nennen. Ein solches Feedback kann jedoch nur dann die Verwendung pseudonymer statt anonymer Daten rechtfertigen, wenn die Rückmeldung mit den Patienten im Rahmen einer hinreichend bestimmten Einwilligung vereinbart wurde (vgl. auch Kap. 4.4.2). Auch die zunehmend hochselektive Rekrutierung für neue Studien kann nur mit Hilfe pseudonymisiert gespeicherter Daten unterstützt werden. Siehe hierzu auch Kapitel 3.2.3.

4.2.5 Elektronische Datentreuhänderschaft

Die vorliegende Konzeption datenschutzgerechter Lösungen in der medizinischen Forschung sieht für viele Szenarien 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. Die Einbindung eines Treuhänders bedeutet, dass die Verwaltung und Speicherung dieser Informationen bei einer Einrichtung oder Person angesiedelt wird, die rechtlich, räumlich und personell selbstständig und unabhängig ist. Darüber hinaus sollte der Treuhänder auch das Vertrauen der betroffenen Patienten oder Probanden genießen.

Da schon allein die Tatsache, dass ein Patient mit Namen und Anschrift oder anderen identifizierenden Daten in einer solchen Liste gespeichert ist, etwas über eine spezifische Erkrankung des Patienten aussagen kann, sind auch solche Daten als sensibel und schützenswert einzustufen. In besonderen Fällen kann der begründete Wunsch der Probanden bestehen, dass eine solche zentrale Datei beschlagnahmesicher im Sinne des § 97 StPO aufbewahrt wird. Vor diesem Hintergrund wurde in der Vergangenheit für einige Forschungsnetze die Beauftragung eines Notars als Datentreuhänder vorgeschlagen [19, S. 41] und z.T. auch umgesetzt, so z.B. im Kompetenznetz Parkinson[13].

Der von der TMF zur Klärung der Rahmenbedingungen einer elektronischen Datentreuhänderschaft beauftragte Rechtsgutachter Dierks weist zum einen auf das vom Beschlagnahmeschutz und dem komplementären Zeugnisverweigerungsrecht nach § 53 StPO adressierte Verhältnis zwischen Arzt und Patient und zum anderen auf die Thematik des Gewahrsams hin. Beide Aspekte, sowohl das Vertrauensverhältnis als zu schützendes Gut und Ausgangspunkt des Beschlagnahmeschutzes, als auch die Regelungen zum Gewahrsam, können sich für die Forschung als problematisch erweisen [20].

Nach Dierks [20, S. B12] ist zwar davon auszugehen, dass auch ein forschender Arzt zu dem Kreis der potenziell Zeugnisverweigerungsberechtigten des § 53 Abs. 1 Nr. 3 StPO gehört. Das Zeugnisverweigerungsrecht steht ihm jedoch nur zu, soweit es um Informationen geht, die ihm in seiner Eigenschaft als Arzt vom Hilfesuchenden anvertraut worden oder bekannt geworden sind. Maßgeblich ist somit das individuelle Beratungs- und Behandlungsverhältnis zwischen dem Arzt und demjenigen, der seine Hilfe in Anspruch nimmt. Ein forschender Arzt, der kein individuelles Beratungs- oder Behandlungsverhältnis zum Patienten hat, wird sich in einem Strafverfahren im Regelfall nicht auf ein Zeugnisverweigerungsrecht berufen können. In den Fällen, in denen die Forschung im Rahmen eines Behandlungsverhältnisses stattfindet, wie

13 www.kompetenznetz-parkinson.de

dies z.B. im Rahmen klinischer Prüfungen zumeist anzunehmen ist, kann aber auch für den forschenden Arzt ein Zeugnisverweigerungsrecht angenommen werden. Analog kann von einem Zeugnisverweigerungsrecht ausgegangen werden, 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 oder beratenden Arztes nach § 53a StPO, sondern selbst zeugnisverweigerungsberechtigt im Sinne des § 53 Abs. 1 Nr. 3 StPO.

Neben dem individuellen Beratungs- und Behandlungsverhältnis zwischen Arzt und Patient sind aber auch die Regelungen zum Gewahrsam der zu schützenden Daten zu berücksichtigen. Eine relevante Erweiterung der Regelungen zum Gewahrsam wurde im Rahmen des Gesetzes zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz – GMG) im Jahre 2003 zur Vorbereitung der Einführung der elektronischen Gesundheitskarte (eGK) eingeführt. Seitdem können Daten auch im Gewahrsam eines Dienstleisters des zeugnisverweigerungsberechtigten Arztes vom Beschlagnahmeschutz umfasst sein. Dierks weist darauf hin, dass der Begriff des Dienstleisters im konkreten Zusammenhang mit der Einführung der eGK und der zugehörigen Telematikinfrastruktur im Gesundheitswesen im Gesetz verankert wurde, dass er aber dem Wortlaut des Gesetzes nach auch unabhängig von der eGK verstanden werden kann und sollte. Demnach wären auch Daten bei einem Dienstleister von einer Beschlagnahme ausgenommen, wenn dessen Beauftragung unabhängig von der Nutzung einer eGK wäre. Vor dem Hintergrund der aktuell eingeschränkten Nutzbarkeit der eGK-Infrastruktur für die Forschung (s. das weiter unten folgende Kap. 4.3.2 zur Gesundheitstelematik) kann dieser Befund für einige Anwendungsfälle der Forschung von Interesse sein. Dierks weist aber auch darauf hin, dass es derzeit zur Interpretation des Dienstleisters nach § 97 Abs. 2 Satz 2 StPO noch keine ausreichend umfangreiche Rechtsprechung gibt, die einen verlässlichen Rechtsrahmen aufspannen würde [20, S. B18].

Somit wäre ein Beschlagnahmeschutz in vertretbarer, jedoch rechtlich nicht abgesicherter Weise über die Aufbewahrung der Patientenliste in elektronischer Form bei einem IT-Dienstleister nach § 97 Abs. 2 Satz 2 StPO zu erreichen, sofern ein eindeutiger Bezug zum spezifischen geschützten Vertrauensverhältnis zwischen Arzt und Patient gegeben ist, aus dem die Daten stammen. Allerdings würde in einem solchen Falle der Dienstleister eine Datenverarbeitung im Auftrag (vgl. § 28 BDSG) übernehmen und wäre gegenüber dem Auftraggeber weisungsgebunden. Metschke und Wellbrock weisen jedoch darauf hin, dass bei einer Datenverarbeitung im Auftrag aufgrund der Weisungsgebundenheit des Auftragnehmers keine ausreichende informationelle Gewaltenteilung erreicht wird. Hierfür muss der Datentreuhänder selbstständige Daten besitzende Stelle sein [19, S. 42]. Die informationelle Gewaltenteilung ist im Regelfall jedoch gerade das Ziel der Einbindung eines Datentreuhänders.

Zu der Frage, ob ein weitergehender Beschlagnahmeschutz durch die Einschaltung eines Notars als Datentreuhänder erreicht werden kann, kommt Dierks allerdings zu einem negativen Ergebnis. Zwar gehören Notare auch zu dem zeugnisverweigerungsberechtigten Personenkreis nach § 53 (1) StPO, allerdings dürfen sie nur über jene Begebenheiten das Zeugnis verweigern, die ihnen in ihrer beruflichen Eigenschaft von ihren Mandanten anvertraut wurden oder bekannt geworden sind und somit das spezifische Vertrauensverhältnis zwischen ihnen und dem auftraggebenden Mandanten betreffen. Informationen über Dritte sind davon nicht automatisch umfasst. Nach Dierks gehört weder die beschlagnahmesichere Aufbewahrung von Dokumenten an sich zu den vom Beschlagnahmeschutz umfassten beruflichen Tätigkeitsbereich eines Notars, noch könnte eine Patientenliste in einem rechtlich sinnvollen Auftrags- und Mandantenverhältnis bei einem Notar so hinterlegt werden, dass dieser sich auf sein Zeugnisverweigerungsrecht berufen könnte. Selbst wenn die Patienten einzeln den Notar mit der Verwaltung ihrer Daten beauftragen würden, müssten sie doch gleichzeitig zur Ermöglichung eines zentralen Zugriffs durch das Forschungsnetz den Notar von seiner Schweigepflicht diesbezüglich entbinden, was wiederum auch die Beschlagnahmesicherheit unterminieren würde. Für Dierks spricht schließlich der Umstand, dass die Mandatierung des Notars gerade der Erreichung eines Beschlagnahmeschutzes dienen soll, für die Beschlagnahmefähigkeit einer Patientenliste beim Notar. Die Übergabe der Patientenliste in die notarielle Verwahrung betrifft dann nicht den Gegenstand seiner typischen und speziellen beruflichen Tätigkeit. Es ist vielmehr von einem Umgehungstatbestand auszugehen, der durch den Schutzzweck des § 97 StPO nicht gedeckt ist [20, S. B22f].

In der Konsequenz ist eine beschlagnahmesichere Einschaltung eines Datentreuhänders in der Forschung nur in wenigen, überwiegend monozentrischen Szenarien erreichbar. Zudem wird in einer solchen Konstellation aufgrund der notwendigen Weisungsgebundenheit des Treuhänders das Prinzip der informationellen Gewaltenteilung durchbrochen. Die Nutzung eines Datentreuhänders ist in vielen Anwendungsfällen und Forschungsfeldern, in denen die Beschlagnahmesicherheit kein hoch priorisiertes Kriterium ist, durchaus sinnvoll und im Sinne einer informationellen Gewaltenteilung positiv zu bewerten. Dies gilt insbesondere dann, wenn es gelingt, eine Institution oder Person für diese Aufgabe zu gewinnen, die bei der relevanten Patientengruppe hohes Vertrauen genießt. Zudem sollte eine solche Stelle datenschutzrechtliche Kompetenz aufweisen und idealerweise auch durch berufsrechtliche Normen an einen vertrauensvollen und sicheren Umgang mit den anvertrauten Daten gebunden sein, wie dies z.B. für Ärzte oder auch Notare gilt.

4.3 Weitere rechtliche Rahmenbedingungen

4.3.1 AMG, MPG

Das Arzneimittelrecht legt in Deutschland die Rahmenbedingungen für klinische Prüfungen fest, die den Nutzen und die Sicherheit eines neuen Medikaments oder der Erweiterung des Anwendungsbereichs eines bekannten Medikaments vor der breiten Anwendung belegen müssen. Analog finden sich Regelungen für die Durchführung klinischer Prüfungen im Rahmen der Bewertung neuer Medizinprodukte im Gesetz über Medizinprodukte (MPG) und der zugehörigen Verordnung über klinische Prüfungen von Medizinprodukten (MPKPV). 2009 wurde eine grundlegende Überarbeitung des MPG verabschiedet, die u.a. die Regelungen zu klinischen Prüfungen mit denen des Arzneimittelrechts vereinheitlichen sollte. Hinsichtlich einiger datenschutzrelevanter Aspekte wurde dieses Ziel jedoch verfehlt, so dass auf diese gesondert in diesem Kapitel eingegangen wird.

Das Gesetz über den Verkehr mit Arzneimitteln (Arzneimittelgesetz – AMG) wurde 2004 dahingehend grundlegend erweitert, dass es nicht mehr nur klinische Prüfungen im Rahmen einer kommerziell relevanten Zulassung regelt, sondern auch den Rechtsrahmen für wissenschaftlich motivierte Arzneimittelstudien bildet. Seit dieser 12. AMG-Novelle ist somit das Risiko der Probanden, welches mit der Anwendung eines neuen Arzneimittels oder dessen Anwendungserweiterung einhergeht, das entscheidende Kriterium für die Anwendbarkeit des Rechtsrahmens des AMG. Somit ist das AMG seit 2004 auch für einen Großteil der öffentlich geförderten klinischen Forschung relevant. Den immensen zusätzlichen Aufwänden, vom Studium und Verständnis der Regelungen bis hin zur Implementierung und regelmäßigen Überprüfung, stehen vor allem Sicherheits- und Qualitätsgewinne gegenüber.

Das AMG wurde seit 2004 mehrmals überarbeitet. Im Folgenden wird der Stand nach der 15. Novelle aus dem Jahr 2009 reflektiert, der allerdings hinsichtlich der Regelungen zum Datenschutz kaum Änderungen gegenüber der Fassung aus 2004 aufweist. Dieser Stand entspricht weitgehend auch einer nationalen Umsetzung der EU-Richtlinie 2001/20/EG. Auch für den Bereich des Arzneimittelrechts ist jedoch schon eine weitere europäische Vereinheitlichungsinitiative gestartet worden [21][14].

Aus Sicht des Datenschutzes sind insbesondere die Regelungen im AMG zur verpflichtenden Pseudonymisierung der erhobenen Daten im sechsten Ab-

14 Die neue „Verordnung des Europäischen Parlaments und des Rates über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG" ist am 27.05.2014 als EU-Verordnung 536/2014 im Amtsblatt der Europäischen Union veröffentlicht worden. Die Verordnung ist am 16. Juni 2014 in Kraft getreten und gilt, abhängig von den bis dahin zu schaffenden Rahmenbedingungen, frühestens ab dem 28. Mai 2016. Sie wird dann die jeweils nationalen Regelungen zur Durchführung klinischer Arzneimittelstudien weitgehend ersetzen (s. http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32014R0536).

schnitt zum „Schutz des Menschen bei der klinischen Prüfung“ sowie im vierten Abschnitt der zugehörigen GCP-Verordnung zu den Dokumentations- und Mitteilungspflichten von Interesse. Demnach sind die Daten innerhalb einer klinischen Prüfung insbesondere dem Sponsor nur in pseudonymisierter Form zur Verfügung zu stellen. Wenn die klinische Prüfung von einem industriellen Sponsor initiiert und verantwortet wird, so kann davon ausgegangen werden, dass dieser in aller Regel kein Interesse daran haben wird, die betroffenen Personen namentlich zu kennen. Somit setzt die Pseudonymisierungsverpflichtung lediglich das Prinzip der Datensparsamkeit aus dem Datenschutzrecht um. Gemäß § 40 Abs. 2a Satz 2 Nr. 1b AMG sind die Probanden einer klinischen Prüfung darüber zu informieren, dass die erhobenen Daten soweit erforderlich pseudonymisiert an den Sponsor oder eine von diesem beauftragte Stelle zum Zwecke der wissenschaftlichen Auswertung weitergegeben werden. Die Einwilligung in die pseudonymisierte Weitergabe der Daten erstreckt sich nach Satz 2 Nr. 1d auch auf die Verpflichtung der Meldung unerwünschter Ereignisse an den Sponsor, die zuständige Bundesoberbehörde und über diese an die hierfür eingerichtete europäische Datenbank. Entsprechende Hinweise darauf wie auch auf eingeschränkte (Satz 2 Nr. 3) oder fehlende Widerrufsmöglichkeiten (Satz 2 Nr. 2) sind in die Aufklärungs- bzw. Einwilligungsformulare aufzunehmen.

Die Regeln des AMG zur Pseudonymisierung sind so weit nachvollziehbar und entsprechen einer datenschutzgerechten Umsetzung. Im Sonderfall einer wissenschaftlich motivierten und initiierten Prüfung (Investigator Initiated Trial – IIT) ist jedoch zu beachten, dass Sponsor und Prüfer einer Studie identisch sein können. Für den Leiter der klinischen Prüfung wird dies regelmäßig gelten. Somit gibt es Konstellationen, in denen die personenbezogenen Daten für den Sponsor ohne weiteres jederzeit einsehbar oder ihm bekannt sind, da er zugleich diejenige Stelle ist, die die klinische Prüfung durchführt. Damit hat der Sponsor, soweit er gleichzeitig Prüfer ist, ohnehin jederzeit unbeschränkten direkten Zugriff auf die ihm gegenüber gem. § 40 Abs. 2a S. 2 Nr. 1b AMG grundsätzlich zu pseudonymisierenden Daten. In einem von der TMF in Auftrag gegebenen Gutachten kommt Dierks zu dem Schluss [22, S. B12], dass in diesen Fällen das Pseudonymisieren unter Betrachtung von Sinn und Zweck der gesetzlichen Vorschriften nicht erforderlich ist. Den Pflichten des Prüfers zur Übermittlung pseudonymisierter Daten an den Sponsor im Rahmen der Meldepflichten nach § 12 Abs. 4, 5 und 6 GCP V kommt aufgrund der Personenidentität von Prüfer und Sponsor bei IITs keine Bedeutung zu. Allerdings sind die Daten in IITs dann pseudonymisiert an den Sponsor zu übermitteln, wenn der Sponsor im Rahmen multizentrischer Studien nicht identisch mit der durchführenden Stelle bzw. dem konkreten Prüfer ist und somit auch nicht über Zugang zu den identifizierenden Daten der betroffenen Probanden verfügt.

Anders als im AMG finden sich in den Bestimmungen zu klinischen Prüfungen im MPG und in der MPKPV keine konkreten Vorschriften zu einer Pseudonymisierung von Daten. Die Umsetzung des datenschutzrechtlichen Prinzips

der Datensparsamkeit gebietet jedoch im Regelfall ebenfalls eine Pseudonymisierung der Daten, wenn diese außerhalb des Behandlungskontextes verarbeitet werden. Insofern wird die erstaunliche Unterschiedlichkeit der gesetzlichen Formulierungen diesbezüglich in der praktischen Umsetzung kaum Konsequenzen haben. Ein weiterer und für die Praxis relevanter Unterschied findet sich in den Vorgaben für die Einwilligungserklärungen: Die im AMG festgelegte Unwiderruflichkeit der Datenverarbeitung fehlt in den Bestimmungen des MPG. Vielmehr wird in § 20 Abs. 2 MPG explizit die jederzeit mögliche Widerrufbarkeit aufgeführt. Da dies dem datenschutzrechtlichen Standard entspricht, ergeben sich daraus im Vergleich zu Forschungsprojekten außerhalb des Regelungsbereichs von AMG und MPG keine Besonderheiten.

4.3.2 Gesundheitstelematik

Die langfristige Sammlung von Patientendaten auf nationaler Ebene, wie sie z.B. von den Kompetenznetzen in der Medizin zu wissenschaftlichen Zwecken seit jetzt über zehn Jahren betrieben wird, weist als Anwendungsfall viele Parallelen zu einigen der geplanten Anwendungen der im Aufbau befindlichen Telematikinfrastruktur auf Basis der elektronischen Gesundheitskarte (eGK) auf. So soll die eGK gemäß § 291a Abs. 3 Satz 1 Nr. 4 SGB V „... insbesondere das Erheben, Verarbeiten und Nutzen [...] von Daten über Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte sowie Impfungen für eine fall- und einrichtungsübergreifende Dokumentation über den Patienten (elektronische Patientenakte) ...“ unterstützen. Demnach wäre eine elektronische Patientenakte (EPA) nach § 291a SGB V hinsichtlich der zu speichernden Daten, der vorgesehenen Dauer der Speicherung und des Verwendungszwecks z.T. durchaus vergleichbar mit dem Modell der Bereitstellung von Behandlungs- und Forschungsdaten in klinisch fokussierten Forschungsnetzen, wie es in der ersten Version der generischen Lösungen zum Datenschutz der TMF beschrieben wurde [1]. Im vorliegenden Konzept ist dieses Modell in Kapitel 5.1 zum Klinischen Modul weiterentwickelt worden. Aber auch die in § 291a Abs. 3 Satz 1 Nr. 5 SGB V vorgesehene Bereitstellung von Daten durch Versicherte selbst stellt einen für die Forschung zunehmend relevanten Anwendungsfall dar.

Bei diesen Überschneidungen der Ansätze und Interessen aus der Forschung mit denen aus der Versorgung liegt die Frage nach gemeinsamen Verwendungsmöglichkeiten einer einheitlichen Infrastruktur nahe. Nach § 291a Abs. 8 Satz 1 SGB V darf jedoch vom Inhaber der eGK nicht verlangt werden, einen Zugriff u.a. auf die Daten nach Abs. 3 Satz 1 „... zu anderen Zwecken als denen der Versorgung der Versicherten ...“ zu gestatten oder eine Gestattung mit ihm zu vereinbaren. In ihrem Gutachten kommen Roßnagel, Hornung und Jandt [11] entsprechend auch zu dem Schluss, dass eine rechtfertigende Einwilligung des Patienten in einen Zugriff auf die auf oder mittels der eGK gespeicherten Daten, die für die Nutzung zu Forschungszwecken notwendig wäre, jenseits der genannten Zwecke ausgeschlossen ist. Dies gilt ebenfalls für zusätzliche,

z.B. im Rahmen klinischer Studien erhobene Daten, wenn diese auf oder mit Hilfe der eGK gespeichert werden. Auch die von Patienten gemäß § 291a Abs. 3 Satz 1 Nr. 5 SGB V selbst in einem so genannten „Patientenfach" zur Verfügung gestellten Daten wären von diesem Verwendungsvorbehalt betroffen. Im Ergebnis ist damit eine Nutzung für die Forschung, auch als zusätzliche Funktion der Gesundheitskarte, nach geltendem Recht unzulässig.

Nach Roßnagel, Hornung und Jandt [11] ist ebenfalls die Nutzung der neuen Versichertennummer der eGK als identifizierendes Merkmal der Patienten im Forschungskontext unzulässig. Dies wäre für einrichtungsübergreifende Forschungsfragestellungen aufgrund des versicherungsunabhängigen und lebenslang gültigen Anteils der neuen Versichertennummer von Interesse und würde helfen, Patienten z.B. auch nach einem Namenswechsel eindeutig zuzuordnen. Nach Aussage der Gutachter ist das Verwendungsverbot unabhängig davon, ob die Versichertennummer direkt oder in nachvollziehbarer Weise umgeschlüsselt als Pseudonym genutzt wird, oder ob sogar nur eine Verwendung als identifizierendes Datum entsprechend der Vorgaben zum ID-Management in einem Forschungsverbund, wie in Kapitel 6.1.1.1 beschrieben und z.B. mit dem PID-Generator der TMF umsetzbar, geplant sei. Hintergrund dieser Einschätzung der Gutachter ist das bereits weiter vorne ausführlich erläuterte BSG-Urteil vom 10.12.2008 [12], welches die Verwendung von Sozialdaten aus dem zehnten Kapitel des SGB V zu nicht im SGB spezifizierten Zwecken auch bei Vorliegen einer Einwilligung ausschließt.

Nicht ausgeschlossen ist aber die Nutzung anderer Komponenten der im Aufbau befindlichen Telematikinfrastruktur, wie z.B. des Heilberufeausweises (HBA) zur einheitlichen und einrichtungsübergreifenden Authentifizierung der Nutzer zentraler IT-Infrastruktur-Komponenten der Forschungsnetze oder von Mehrwertdiensten (s. Glossar).

4.3.3 Eigentumsrecht bei Biomaterialien

Als weiterer relevanter Rechtsrahmen ist für biologische Proben das Sachenrecht nach § 854–1296 BGB zu berücksichtigen. Zwar gilt der menschliche Körper oder auch ein einzelnes Körperteil oder abgetrenntes Körpermaterial nicht als Sache im gesetzlichen Sinne. Für abgetrennte Körperteile oder Körpermaterialien wie Gewebe, Blut etc. trifft dies jedoch zunächst nur zu, wenn eine Wiedereingliederung geplant ist, wie z.B. bei einer Eigenblutspende oder einer Organtransplantation. Proben in Biomaterialbanken für die Forschung sind jedoch durchweg Körpermaterialien, die eindeutig ohne Absicht und Möglichkeit der Wiedereingliederung entnommen worden sind. Damit sind sie als Sachen im Sinne des § 90 BGB einzuordnen [23, S. 32].

Das auf das Sachenrecht zurückgehende Eigentumsrecht steht grundsätzlich und ohne weitere Vereinbarung den Spendern zu. Dabei wird das Eigentumsrecht an den Proben vom allgemeinen Persönlichkeitsrecht überlagert, wobei

die Intensität dieser Überlagerung davon abhängt, in welchem Umfang Rückschlüsse vom Körpermaterial auf dessen ehemaligen Träger und seine Person gezogen werden können. Nur wenn solche Rückschlüsse nicht mehr möglich sind, wäre das allgemeine Persönlichkeitsrecht bedeutungslos. Das im Regelfall anzunehmende Persönlichkeitsrecht, wie auch das in Verbindung damit stehende Widerrufsrecht der Probanden schließen eine implizite Eigentumsübertragung im Rahmen der Einwilligung in die Teilnahme an einem Forschungsprojekt üblicherweise aus [23]. Eine explizite Eigentumsübertragung ist aber nach allgemeiner Auffassung möglich, auch wenn die Persönlichkeitsrechte an der Probe nicht übertragbar sind und damit notwendigerweise von der Eigentumsübertragung unberührt bleiben [5, S. 118]. Wenn ein Verwertungsbedarf in Bezug auf die Proben nicht ausgeschlossen werden kann, sollten die Probanden entsprechend explizit um eine Eigentumsübertragung gebeten werden. Als weiterführende Lektüre zu diesem Themenkomplex wird auf das im Auftrag der TMF erstellte Rechtsgutachten von Simon und Mitarbeitern verwiesen, welches als Band 2 der Schriftenreihe der TMF veröffentlicht wurde [23].

4.3.4 Abgleich mit externen Datenbeständen

Gerade in epidemiologischen Forschungsprojekten kann ein berechtigtes Interesse an Datenübermittlungen von beispielsweise Einwohnermelde-, Gesundheits- oder Standesämtern bestehen. Die gesetzlichen Grundlagen für die Übermittlung von Daten aus Melderegistern stehen typischerweise in den Meldegesetzen der Länder. So erlaubt z.B. § 31 Abs. 1 des Meldegesetzes für Rheinland-Pfalz den Meldebehörden die Übermittlung bestimmter Daten an andere Behörden oder öffentliche Stellen, soweit dies zur Erfüllung von Aufgaben erforderlich ist, die in ihrer Zuständigkeit oder der der empfangenden Stelle liegen. Regelungen für die Standesämter finden sich hingegen im Personenstandsgesetz (PStG). Für einige Forschungsprojekte ist auch eine genaue Kenntnis der Todesursachen verstorbener Patienten notwendig. Solche Daten können in bestimmten Fällen von den Gesundheitsämtern angefordert werden. Den gesetzlichen Rahmen für solche Informationsübermittlungen spannen die Gesundheitsdienstgesetze der Länder auf. Eine weitere relevante Datenquelle können die Krebsregister auf Landesebene sein, für die in den Landeskrebsregistergesetzen die Bedingungen für eine Datenweitergabe zu Forschungszwecken festgehalten sind.

4.4 Patientenrechte

4.4.1 Auskunftsrechte

Jeder Proband hat nach § 34 (1) BDSG ein grundsätzliches Recht auf Auskunft über die von ihm gespeicherten personenbezogenen Daten, also auch über abgeleitete oder aus Biomaterialien gewonnene Daten. Zu dieser Auskunfts-

pflicht gibt es in § 33 (2) BDSG aufgezählte Ausnahmen, wie etwa ein unverhältnismäßiger Aufwand, die Geheimhaltungspflicht aufgrund einer Rechtsvorschrift oder wegen des überwiegenden rechtlichen Interesses eines Dritten, die Gefährdung der öffentlichen Sicherheit oder Ordnung oder eine erhebliche Gefährdung der Geschäftszwecke der verantwortlichen Stelle, die jedoch in der Regel auf die hier behandelten Daten- und Probensammlungen der Forschung nicht zutreffen. Die Möglichkeit der Auskunft besteht nur, solange die Daten nicht anonymisiert wurden. Korrespondierend zu den Auskunftsrechten besteht nach § 35 BDSG das Recht der Probanden auf Berichtigung, Löschung oder Sperrung ihrer Daten.

4.4.2 Recht auf Wissen und Nichtwissen

An den Ergebnissen medizinischer Forschung können Probanden ein berechtigtes Mitteilungsinteresse haben, insbesondere dann, wenn es sich um individuelle Untersuchungsergebnisse mit medizinischer Relevanz handelt. Die Möglichkeit der Entstehung solcher Ergebnisse kann gerade bei Nutzung umfangreicher Daten- und Probensammlungen immer seltener von vornherein ausgeschlossen werden. Vor diesem Hintergrund sollten die Probanden im Vorfeld über mögliche Untersuchungsergebnisse aufgeklärt und mit ihnen eine entsprechende Auskunftsregelung vereinbart werden. Dabei ist allerdings auch zu berücksichtigen, dass Probanden bestimmte Untersuchungsergebnisse möglicherweise nicht mitgeteilt bekommen möchten. Dies kann z.B. auf Ergebnisse aus genetischen Untersuchungen oder andere Befunde mit prädiktivem Charakter zutreffen. Auch diesem Recht auf Nichtwissen ist in entsprechenden Vereinbarungen Rechnung zu tragen [vgl. 24; 25]. In diesem Zusammenhang sind Probanden zudem darauf hinzuweisen, dass sie ihnen bekannte Untersuchungsergebnisse ggf. auch Versicherungen oder Arbeitgebern mitteilen müssen. Zum anderen können Ergebnisse aus genetischen Untersuchungen auch eine Relevanz für Angehörige des Probanden aufweisen, so dass deren Recht auf Nichtwissen auch zu berücksichtigen ist. Sollte ein Proband darauf bestehen, über die Ergebnisse der genetischen Untersuchungen informiert zu werden, so kann ihm das aufgrund seines informationellen Selbstbestimmungsrechts nicht versagt werden. Er kann jedoch dann selbst in den Konflikt geraten, einerseits Angehörige darüber informieren zu wollen, dass relevante Informationen aus genetischen Untersuchungen vorhanden sind, andererseits aber auch deren Recht auf Nichtwissen respektieren zu müssen. Auf eine solche mögliche Konfliktsituation sollten Probanden daher im Vorfeld hingewiesen werden [weitere Informationen hierzu in: 5, S. 78].

Bei der Festlegung eines Standardverfahrens, von welchem im Rahmen abgestufter Einwilligungserklärungen in vordefinierter Form auch abgewichen werden kann, sollte berücksichtigt werden, dass gerade viele Zufallsbefunde aus genetischen oder anderen Untersuchungen bei geringer tatsächlicher Relevanz für die Probanden doch gleichzeitig auch erhebliches Verunsicherungs-

potenzial besitzen können. Zudem ist der Aufwand der Informierung der Probanden nicht zu unterschätzen, da zum einen möglicherweise auch Beratungskompetenz mit zur Verfügung gestellt und zum anderen die notwendige Depseudonymisierung mit allen damit verbundenen Komplikationen geregelt werden muss. Hinsichtlich der Depseudonymisierung ist an ggf. notwendige Entbindungen von der Schweigepflicht zu denken oder es müssen technische und organisatorische Verfahren implementiert werden, die sicherstellen, dass nur der behandelnde Arzt den Untersuchungsbefund in depseudonymisierter Form erhält.

Vor dem Hintergrund der genannten Aufwände und der möglicherweise in vielen Fällen geringen Relevanz der Mitteilung von Zufallsbefunden kann ein Forschungsprojekt auch vorsehen, dass die Probanden mit der Einwilligungserklärung auf ein Mitteilungsrecht zunächst verzichten. Dies kann auch zur Bedingung einer Teilnahme am Forschungsprojekt gemacht werden [14]. Allerdings ist zu beachten, dass Probanden diese Vereinbarung auch widerrufen können und ihnen das Auskunftsrecht dann zu einem späteren Zeitpunkt doch zusteht. Ein unwiderruflicher Verzicht auf Mitteilung von Untersuchungsergebnissen kann nicht mit den Probanden vereinbart werden.

Ein vereinbarter Verzicht auf die Mitteilung von Ergebnissen kann in bestimmten Fällen die spätere Rekrutierung von Probanden einschränken. Dies kann z.B. der Fall sein, wenn für eine Präventionsstudie überwiegend oder ausschließlich Patienten rekrutiert werden sollen, die bestimmte Risikofaktoren aufweisen und der vereinbarte Mitteilungsverzicht impliziert, dass der Proband über das Vorhandensein eines solchen Risikofaktors nicht informiert wird.

Von den Auskunftsrechten der Patienten sind u.U. ärztlich begründete Mitteilungspflichten der Forscher zu unterscheiden. Diese beziehen sich z.B. auf wichtige medizinische Befunde mit unmittelbaren Konsequenzen für eine weitere Behandlung oder Diagnostik. Der hierfür nötige Regelungsumfang entspricht weitgehend jenem für die Auskunftsrechte der Probanden. Die entsprechenden Vereinbarungen können somit analog formuliert werden. Grundsätzlich ist zu beachten, dass alle genannten Auskunftsrechte der Patienten und Mitteilungspflichten der Forscher sich nur auf Daten beziehen, die nicht anonymisiert wurden [5, S. 132].

4.4.3 Einbeziehung von Ethikkommissionen

Die Berücksichtigung der vorliegenden Empfehlungen zur datenschutzgerechten Umsetzung medizinischer Forschungsprojekte kann und soll die sorgfältige Beratung und Prüfung eines Forschungsprojekts in jedem Einzelfall durch eine oder mehrere Ethikkommissionen nicht ersetzen. Eine berufsrechtliche Pflicht, sich durch eine Ethikkommission beraten zu lassen, ergibt sich aus den Regelungen der Berufsordnungen. Dies gilt immer dann, wenn im Rah-

men eines Forschungsprojekts in die psychische oder körperliche Integrität eines Menschen eingegriffen wird oder personenbezogene Proben oder Daten verwendet werden (§ 15 MBO). Für Forschungsvorhaben im Anwendungsbereich des Arzneimittelrechts ist eine Prüfung gemäß § 40 (1) AMG verpflichtend, gleiches gilt für nach Medizinproduktegesetz geregelte klinische Prüfungen (§ 20 [7] MPG). Gleichwohl soll der hier vorgelegte konzeptionelle Rahmen die Überprüfung von Forschungsprojekten in Bezug auf datenschutzrechtliche Fragen durch Ethikkommissionen vereinfachen und verbessern helfen. Gerade die Abstimmung und Prüfung einrichtungsübergreifender und auf Langfristigkeit angelegter Datensammlungen mit ihren entsprechend aufwändigen Schutzprinzipien wird von einem allseits anerkannten Bezugsrahmen profitieren und beschleunigt werden.

Die Prüfung datenschutzrechtlicher Aspekte betrifft zudem nur einen Teil des Aufgabenspektrums der Ethikkommissionen. Ihr Auftrag umfasst die Prüfung der medizinischen Forschung am Menschen aus ethischer, rechtlicher und sozialer Sicht und geht wesentlich auf die Deklaration von Helsinki zurück [26]. So ist beispielsweise bei interventionellen Studien das Studiendesign daraufhin zu prüfen, ob alle schonenderen oder weniger riskanten Untersuchungsmöglichkeiten sorgfältig erwogen und begründet ausgeschlossen wurden. Andererseits ist auch abzuklären, ob das gewählte Studiendesign samt vorgesehener Stichprobengröße überhaupt zu Ergebnissen führen kann, die das Risiko für jeden einzelnen Patienten rechtfertigen. Schließlich sind die Aufklärungs- und Einwilligungsformulare zu begutachten, was wiederum auch datenschutzrechtliche Aspekte betrifft.

4.5 Ebenen des Datenschutzrechts und der Datenschutzaufsicht

Viele Forscher stehen zu Beginn der datenschutzrechtlichen Klärung ihres Projekts vor zwei Fragen: Welches Datenschutzgesetz gilt für mein Projekt und welcher Datenschutzbeauftragte ist mein Ansprechpartner? Ein Blick in das virtuelle Datenschutzbüro für Deutschland, angeboten vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD), zeigt, dass es neben dem Bundesdatenschutzbeauftragten und dem Bundesdatenschutzgesetz auch Regelungen und Ansprechpartner für jedes der 16 Bundesländer in Deutschland gibt[15]. Zusätzlich gibt es in öffentlichen Einrichtungen im Regelfall auch noch einen behördlichen und in privat getragenen Einrichtungen ab einer bestimmten Größe einen betrieblichen Datenschutzbeauftragten, der als Ansprechpartner in Frage käme. Wo also anfangen?

Das im vorliegenden Text hauptsächlich referierte Bundesdatenschutzgesetz gilt nach § 1 (2) BDSG für öffentliche Stellen des Bundes und nicht-öffentliche

15 siehe http://www.datenschutz.de/recht/gesetze/

Stellen, also Einrichtungen in privater Trägerschaft. Eingeschränkt gilt es auch für bestimmte Aufgabenbereiche einiger weniger öffentlicher Stellen der Länder. Entsprechend sind die Bestimmungen des Bundesdatenschutzgesetzes in Krankenhäusern in privater Trägerschaft anzuwenden, in Universitätskliniken im Regelfall jedoch nicht, da diese überwiegend öffentliche Einrichtungen der Länder sind. Die datenschutzrechtlichen Belange der öffentlichen Stellen der Länder sind in den Landesdatenschutzgesetzen geregelt[16, 17].

Sowohl auf Landes- wie auf Bundesebene sind in den Datenschutzgesetzen an vielen Stellen die Prinzipien der Europäischen Richtlinie zum Datenschutz 95/46/EG von 1995 umgesetzt. Nicht nur, aber auch aus diesem Grunde sind die Ausführungen an vielen Stellen schon weitgehend harmonisiert, so dass tatsächlich häufig das Bundesdatenschutzgesetz stellvertretend für die Landesdatenschutzgesetze zitiert werden kann. Insofern wäre es auch nicht gerechtfertigt, in Bezug auf das Datenschutzrecht in Deutschland von einem „Flickenteppich" zu sprechen. Unübersichtlich wird die Lage allerdings insofern als das Datenschutzrecht nur subsidiär zu anderen Gesetzen anzuwenden ist. Namentlich die Landeskrankenhausgesetze führen daher effektiv zu unterschiedlichen datenschutzrechtlichen Bedingungen in den Ländern, gerade auch für die Sekundärnutzung klinischer Daten, wie bereits weiter oben ausgeführt. Einen ersten Überblick hierzu haben Schütze und Oemig ausgearbeitet [27], der allerdings z.B. in Bezug auf das Berliner Krankenhausgesetz schon veraltet ist. Aber auch die Landesdatenschutzgesetze unterscheiden sich doch so weit voneinander, dass für ein konkretes Projekt ggf. das relevante Landesrecht detailliert geprüft werden muss. In größeren Projekten mit der Beteiligung mehrerer öffentlicher Einrichtungen wird die Prüfung heute im Regelfall die Gesetze mehrerer Länder umfassen müssen. Die Mühseligkeit eines solchen Unterfangens zeigt sich u.a. darin, dass auch die Datenschützer selbst in ihren Veröffentlichungen eine genaue Prüfung der landesdatenschutzrechtlichen Besonderheiten mitunter vermeiden [z.B. 28, s. Fußnote 26 auf S. 26].

Als direkter Ansprechpartner für ein konkretes Forschungsprojekt kommt der Bundesbeauftragte für den Datenschutz eher selten in Betracht. Dabei ist es unerheblich, ob private oder öffentliche Stellen in das Projekt involviert sind. Ihm obliegt nach § 24 BDSG im Wesentlichen die Aufsicht über die öffentlichen Stellen des Bundes. Die Aufsicht über private Stellen und die öffentlichen Stellen der Länder ist hingegen auf Länderebene geregelt. Für die öffentlichen

16 Spezifische Regelungen der Kirchen zum Datenschutz sind hier nicht weiter berücksichtigt

17 In einigen Landesdatenschutzgesetzen finden sich Hinweise auf die teilweise Anwendbarkeit des BDSG auch für Einrichtungen in öffentlicher Trägerschaft, wenn diese im Wettbewerb mit privat getragenen Einrichtungen stehen, so z.B. in § 3 BayDSG. Eine Teilnahme am Wettbewerb um Behandlungsverhältnisse kann für öffentlich getragene Krankenhäuser im Regelfall angenommen werden. Eine ausführliche und vergleichende Darstellung der landesdatenschutzrechtlichen Rahmenbedingungen für die Sekundärnutzung klinischer Daten findet sich in einem von der TMF in Auftrag gegebenen und ebenfalls in der TMF-Schriftenreihe veröffentlichten Rechtsgutachten.

Stellen ist in den Landesdatenschutzgesetzen die Zuständigkeit der Landesbeauftragten für den Datenschutz (LfD) festgelegt. Die Aufsicht über den privaten Bereich lag bis vor kurzem in den meisten Ländern bei nachgeordneten Behörden der Innenministerien der Länder, z.B. Regierungspräsidien. Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 9. März 2010 festgestellt, dass diese Kontrollstellen in den Bundesländern staatlicher Aufsicht unterstellt sind und damit das Erfordernis gemäß Richtlinie 95/46/EG, dass diese Stellen ihre Aufgaben „in völliger Unabhängigkeit" wahrnehmen, nicht umgesetzt ist [29]. Dieses Urteil hatte in den meisten Bundesländern eine Neuordnung der Datenschutzaufsicht für den privaten Bereich zur Folge, die im Ergebnis in allen Bundesländern bis auf Bayern zu einer erweiterten Zuständigkeit der Landesdatenschutzbeauftragten geführt hat. In Bayern ist das Bayerische Landesamt für den Datenschutz die zuständige Kontrollstelle für nicht-öffentliche Stellen.

Direkter und erster Ansprechpartner könnte in öffentlichen Institutionen der behördliche und in privat getragenen Einrichtungen ab einer gewissen Mindestgröße der betriebliche Datenschutzbeauftragte sein. Die frühzeitige Besprechung von Forschungsvorhaben mit diesen lokalen Ansprechpartnern kann grundsätzlich nur empfohlen werden. Allerdings ist es wichtig zu verstehen, wann darüber hinaus auch die Abstimmung mit den zuständigen Landesdatenschutzbeauftragten angestrebt werden sollte. Die Zuständigkeiten von behördlichem bzw. betrieblichem Datenschutzbeauftragten und dem Landesbeauftragten für den Datenschutz sowie deren Verhältnis untereinander werden im Folgenden exemplarisch für öffentliche Einrichtungen in NRW dargestellt. Diese Ausführungen sollen das komplexe Zusammenspiel der Zuständigkeiten beispielhaft veranschaulichen. Sie lassen sich jedoch nicht direkt auf andere Bundesländer übertragen. Eine Untersuchung der Gegebenheiten in allen Bundesländern würde den Rahmen dieses Leitfadens sprengen. Die TMF plant zu diesem Thema ein Rechtsgutachten einzuholen, welches dann zu einem späteren Zeitpunkt auf der Website der TMF zur Verfügung gestellt wird[18].

Die jeweiligen Aufgaben und Zuständigkeiten sind im Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) festgelegt. Der behördliche Datenschutzbeauftragte hat nach § 32a DSG NRW die Sicherstellung des Datenschutzes in der Einrichtung zu unterstützen. Konkret hat er hierfür insbesondere gemäß § 8 DSG NRW ein lokales Verzeichnis automatisierter Verfahren zur Verarbeitung personenbezogener Daten (Verfahrensverzeichnis) zu führen und gemäß § 32a Absatz 1 Satz 7 DSG NRW Vorabkontrollen durchzuführen. Die Aufgaben und Befugnisse des Landesbeauftragten für Datenschutz und Informationsfreiheit sind in § 22 DSG NRW geregelt. Der Landesbeauftragte ist Aufsichts- und Kontrollbehörde für Datenschutzfragen in NRW. Gemäß § 25 DSG NRW hat jede

18 siehe www.tmf-ev.de/produkte

Person das Recht, sich unmittelbar an ihn zu wenden, wenn er bzw. sie der Ansicht ist, dass gegen datenschutzrechtliche Vorschriften verstoßen worden ist oder ein solcher Verstoß bevorsteht. Der Landesbeauftragte ist zudem gemäß § 4a Absatz 1 Satz 5 DSG NRW über die Errichtung von Verbunddateien und gemäß § 9 Absatz 2 Satz 5 DSG NRW über die Einrichtung automatisierter Abruf- und Übermittlungsverfahren zu unterrichten.

Anfang 2012 hat die Europäische Kommission den Entwurf einer europäischen Datenschutzgrundverordnung (DGVO) vorgestellt [6]. Anders als bei der bisherigen Richtlinie zum Datenschutz, die von den einzelnen Ländern der EU in einem jeweils individuellen Verfahren in nationales Recht umzusetzen war, würde eine solche Verordnung auf europäischer Ebene direkt nationales Recht ersetzen. Damit wäre in weiten Teilen auch eine innerdeutsche Harmonisierung des Datenschutzrechts, sowohl für private wie für öffentliche Stellen, erreicht, was grundsätzlich positiv zu bewerten ist. Zudem enthält der Entwurf in Artikel 83 Regelungen für die Forschung, die eine lokale Nutzung von Daten, vorranging und wenn möglich anonymisiert oder pseudonymisiert, auch ohne Einwilligungserfordernis erlauben würden. Dies könnte zumindest für lokale oder monozentrische Forschungsprojekte eine große Erleichterung bedeuten.

Allerdings wird dieser Entwurf aktuell auf europäischer Ebene und in den Ländern umfassend kommentiert, so dass noch mit einer Reihe von Änderungen zu rechnen ist. Zudem enthält der Entwurf zahlreiche Ermächtigungsklauseln für die Europäische Kommission, delegierte Rechtsakte in Form von Ausführungs- und Konkretisierungsbestimmungen zu erlassen, so auch zu Artikel 83 DGVO. Eine abschließende Bewertung dieser europäischen Gesetzgebungsinitiative ist daher noch nicht möglich.

4.6 Grundprinzipien datenschutzgerechter Lösungen

Der hier dargelegte konzeptuelle Rahmen für datenschutzgerechte Lösungen in der medizinischen Forschung basiert auf einigen elementaren Prinzipien, die im Folgenden zusammengefasst dargestellt sind. Auf ausführlichere Darstellungen zu den einzelnen Prinzipien in anderen Kapiteln wird jeweils verwiesen.

Das **Risiko einer unerlaubten Reidentifizierung** sollte so weitgehend wie möglich und nötig ausgeschlossen werden. Weitere Hinweise zur Verhältnismäßigkeit unterschiedlicher Lösungsansätze finden sich in Kapitel 6.7.

Das Prinzip der **informationellen Gewaltenteilung** sieht vor, dass, wenn möglich und nötig, die gespeicherten identifizierenden Personendaten von den medizinischen Daten getrennt aufbewahrt und verwaltet werden. Im Maximalfall sind hierfür getrennte Institutionen verantwortlich, die keiner gemeinsamen Weisungsbefugnis unterstehen. Zudem kann auch die Verwal-

tung eines Zuordnungsschlüssels in die eigenständige Verwaltung eines unabhängigen Treuhänders gegeben werden. Eine ausführliche Darstellung bietet Kapitel 6.1.

Das Prinzip **sicherer Pseudonyme** ergänzt das Prinzip der informationellen Gewaltenteilung. Pseudonyme sind langfristig sichere, kryptographisch erzeugte Identifikatoren, die nur entlang vorgesehener und rechtmäßiger Verarbeitungs- und Genehmigungsprozeduren eine Reidentifizierung von Probanden ermöglichen. Weitere Informationen sind in Kapitel 6.1 zum ID-Management zu finden.

Das Prinzip der sorgfältigen **Abwägung zwischen Anonymisierung und Pseudonymisierung** erfordert eine genaue Kenntnis der Anwendungsfälle und Nutzungsszenarien. Das Gros der hier dargestellten Anwendungsfälle erfordert eine langfristige pseudonymisierte Speicherung medizinischer Daten, was neben einer Rechtsgrundlage der strikten organisatorischen Einhegung samt effektiver Zugangskontrolle bedarf. Andererseits ist bei anonymisierten Daten immer zu beachten, wie sicher und dauerhaft eine Reidentifizierung ausgeschlossen werden kann. Eine Verwendung solcher Daten in Public-Use-Files setzt eine nachweisbare Anonymisierung voraus, wie sie z.B. das Konzept der k-Anonymisierung (Erläuterung im Glossar) bietet. Genauere Darstellungen beinhalten das Kapitel 5.3 zu Forschungsdatenbanken und das Kapitel 6.1 zum ID-Management.

Das Prinzip **rechtlich klar und transparent geregelter Verantwortlichkeiten** wird durch eine rechtsfähige Organisationsform eines Forschungsverbunds unterstützt.

Das Prinzip der **Kombination technischer und organisatorischer Sicherheitsmaßnahmen** wird durch parallele und ergänzende Anwendung technischer Vorkehrungen wie z.B. Zugriffsbeschränkungen, kryptographische Transformationen, Logging etc. und organisatorischer Regelungen wie z.B. Standard Operating Procedures, klare Verantwortlichkeiten, Vier-Augen-Prinzip bei wichtigen Entscheidungen usw. umgesetzt und ist für einen hohen Sicherheitsstandard im Regelfall unerlässlich.

Das Prinzip **redundanter Absicherung** führt zu einem Schutz der Daten auch dann, wenn eine Sicherungskomponente ausfällt. Dies kann z.B. ein kurzfristig unsicher gewordenes kryptographisches oder technisches Verfahren sein oder eine unerlaubte Umgehung organisatorischer Regelungen. So wird z.B. empfohlen, medizinische und identifizierende Daten nicht gemeinsam über öffentliche Netze wie das Internet zu übertragen und zusätzlich für eine Verschlüsselung der Inhalte auf dem aktuellen Stand der Technik zu sorgen.

Das Prinzip **möglichst einfacher und ökonomischer Lösungen** setzt eine sorgfältige Analyse des konkreten Anwendungsfalls voraus, so dass eine dem Schutzbedarf angepasste und den Kriterien der Verhältnismäßigkeit genügende Implementierung realisiert werden kann. Eine detaillierte Aufstellung re-

levanter Kriterien für eine Anpassung des Sicherheitsaufwands findet sich in Kapitel 6.7.

Das Prinzip der **bestmöglichen Nutzung** aufwändig und womöglich mit persönlichem Risikoeinsatz der beteiligten Probanden erhobener Daten ist einerseits ein ethisches Gebot, dem jedoch andererseits durch das Prinzip der **informierten Einwilligung** Grenzen gesetzt werden. Die Komplexität des hier vorgestellten konzeptuellen Rahmens für datenschutzgerechte Lösungen resultiert ganz wesentlich aus dem Anliegen, auf Langfristigkeit angelegte, pseudonymisierte Datensammlungen zu ermöglichen, die vergleichsweise zweckoffen für die Forschung genutzt werden können, ohne dass Patienten oder Probanden mit ihrer Einwilligung ein unabsehbares Risiko in Bezug auf den ethischen und datenschutzgerechten Umgang mit ihren Daten eingehen.

Zu dem Prinzip der **informationellen Selbstbestimmung** gehört sowohl das Recht auf Wissen als auch das Recht auf Nichtwissen. Wie sichergestellt werden kann, dass Patienten über ihre Daten und Ergebnisse informiert werden können, ohne ihnen dabei nicht gewünschte Informationen aufzudrängen, ist den einzelnen Kapiteln zu den verschiedenen Anwendungsfällen mit ihren jeweiligen Lösungskonzepten zu entnehmen. Jede Diagnostik, die genetische Informationen offenbart, führt in diesem Zusammenhang allerdings zu komplexen Anforderungen, insbesondere hinsichtlich der informationellen Selbstbestimmung der Angehörigen eines Probanden. Hier ist eine entsprechend detaillierte Analyse möglicher Konflikte unerlässlich und jede einmal gefundene Lösung muss eventuell später an neue Rahmenbedingungen angepasst werden.

Die **Vermeidung von Rollenkonflikten** ist als wichtiges Prinzip bei der Festlegung der Rollen und Rechte in einem Forschungsverbund zu berücksichtigen. Eine genaue Prüfung auf mögliche Rollenkonflikte ist in jedem Forschungsvorhaben unerlässlich, insbesondere sollte jede Umgehung des Prinzips der informationellen Gewaltenteilung ausgeschlossen werden. Weitere Hinweise finden sich in Kapitel 6.2.3.