Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Datenschutzrechtliches Gutachten

Datentreuhänderschaft in der Biobank-Forschung – bdc\Audit
(Biobank Data Custodianship / Audit Methodology and Criteria)
Methoden, Kriterien und Handlungsempfehlungen für die datenschutzrechtliche Auditierung der Datentreuhänderschaft in der Biobank-Forschung

Schlussbericht v1.1

Teilprojekt 2

Kiel, 30. April 2009

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstraße 98 – 24103 Kiel
www.datenschutzzentrum.de – +49 431 988 1200

Rechtliche Ausgestaltung der Datentreuhänderschaft für Biobanken

Inhaltsverzeichnis

1 Einleitung

1.1 Auftrag

Im September 2006 ist das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) vom Bundesministerium für Bildung und Forschung (BMBF) im Verbund mit zwei Kooperationspartnern mit der Studie „Datentreuhänderschaft in der Biobank-Forschung – bdc\Audit“ beauftragt worden. Das Projekt wurde unter der Leitung und Koordination des Forschungsschwerpunktes „Biotechnik, Gesellschaft und Umwelt“ der Universität Hamburg (FSP BIOGUM) sowie in Kooperation mit der Arbeitsgruppe Kommunikationssysteme des Instituts für Informatik der Christian-Albrechts-Universität zu Kiel (CAU Kiel) durchgeführt. Dabei hatte jede beteiligte Stelle ein separates Teilprojekt zu verantworten. Das FSP BIOGUM-Teilprojekt beinhaltet die „Analyse und Klassifikation von Biobanken: Strukturen – Elemente – Prozesse“ (TP-1), das Teilprojekt der CAU Kiel befasst sich mit Auditierungsverfahren und –kriterien für die Biobank-Datentreuhänderschaft (TP-3). Das Teilprojekt des ULD umfasst die „Rechtliche Ausgestaltung der Datentreuhänderschaft für Biobanken“ (TP-2). Projektstart war der 1. Oktober 2006, die Laufzeit der Förderung erstreckte sich über zwei Jahre.

Die Problemstellung und -zielsetzung sind von den Projektpartnern in dem Projektantrag ausformuliert. Zu TP-2 ist ausgeführt:

„Eine wichtige Frage (und zugleich Schnittstelle zu TP-3) besteht in der Klärung des Spannungsverhältnisses zwischen Datenschutz/Geberschutz einerseits und der Forschungsfreiheit andererseits sowie zwischen den direkt an Biobanken Beteiligten und Dritten. Diese Spannungen können über rechtliche, organisatorische und technische Anonymisierungs- und Pseudonymisierungskonzepte aufgelöst werden. Um für die Anwender die nötige Rechtssicherheit zu schaffen, soll im Rahmen des bdc\Audit-Verbundprojektes ein internationaler Rechtsvergleich vorgenommen werden. Anknüpfend an vorliegende rechtsvergleichende Ansätze sollen praktische rechtliche Anforderungen abgeleitet werden, deren Beachtung bei grenzüberschreitenden Projekten Rechtskonformität gewährleistet. Bestehende nationale und internationale Sicherheitsanforderungen werden auf Standardisierungsmöglichkeiten hin untersucht. Einfließen müssen hierbei auch die Auditierungsregelungen, die sowohl im nationalen wie im internationalen Rahmen bestehen bzw. derzeit entwickelt werden. Dabei ist von zentraler Bedeutung, welche Funktionen private Stellen, hoheitliche Datenschutzbeauftragte, Ethik-Kommissionen und die wissenschaftliche Gemeinschaft spielen und welche Funktion bestimmten Transparenzpflichten zukommt.“

Weiter ist in dem Antrag zu TP-2 ausgeführt: „Ergebnis der grundlegenden rechtlichen Bestandsaufnahme wird das Erarbeiten von Kriterienkatalogen sein, die für die Auditierung von Biobanken herangezogen werden können sowie von Verfahrensvorschlägen, wie solche Auditierungen durchgeführt werden können. Dabei werden zu folgenden Themen Antworten gegeben werden:

- inhaltliche Voraussetzungen an Einwilligungen/informed consent,
- formelle und prozedurale Anforderungen an Einwilligungen,
- Anforderungen an den gesetzlichen Verzicht auf Einwilligungen,
- Transparenzverpflichtungen gegenüber den Probengebern,

- Betroffenenrechte der Probengeber (Ansprüche auf Information, Benachrichtigung, Auskunft, Widerspruch, Sperrung, Löschung, materielle Ansprüche)
- Transparenzverpflichtungen gegenüber der Gesundheitsverwaltung/ Wissenschaftsverwaltung/ Auftraggeber/Wissenschaft/Öffentlichkeit,
- rechtlich begründete technisch-organisatorische Anforderungen an die Datensicherheit,
- rechtliche Anforderungen an die Anonymisierung, an Pseudonymisierungskonzepte und technisch-organisatorische Pseudonymisierungsverfahren,
- Abschottungspflichten und Informationspflichten bzw. -rechte gegenüber berechtigten und interessierten Dritten."

1.2 Vorgehensweise

Das ULD hat in Absprache und gemeinsam mit den Projektpartnern Befragungen von Biobanken begleitet und den Verbesserungsbedarf mit erhoben. Die Erfahrungen sind in den Bericht eingeflossen.

Die Projektpartner haben am 4. Juli 2008 unter der Leitung des ULD einen Workshop mit dem Titel „Datenschutzrechtliche Auditierung von Biobanken" durchgeführt, in dem u. a. die bis dahin vorliegenden Ergebnisse der Projektarbeit vorgestellt wurden. Themen waren:

- Systemanalyse von Biobanken: Empirische Befunde zur Ablauf- und Aufbauorganisation
- Materielle und formelle Datentreuhänderschaft in Biobanken: Ergebnisse empirischer Analysen
- Spenderschutz durch Datentreuhänderschaft
- Welche Datenschutzkriterien müssen Biobanken erfüllen? Und wie müssen sie diese Erfüllung erkennbar machen?
- Prozessorientierte Biobank-Modellierung: die Basis für die datenschutzrechtliche Auditierung
- IT-Sicherheit in Biobankprozessen durch Schutzprofile und bewertete De-Identifizierungsverfahren
- Nachhaltigkeit – durch vertrauenswürdige und integre Forschungsinfrastrukturen

Im Anschluss an diese kooperative Zusammenarbeit haben die Projektpartner in jeweiliger alleiniger Verantwortung den Abschlussbericht ihres Teilprojektes erstellt.

1.3 Aufbau des Berichts

Biobanken verfügen über eine große Heterogenität, die auch durch TP-1 aufgezeigt und nachgewiesen wird. Ziel des Berichts ist es, eine übergreifende Grundlage für eine datenschutzgerechte Ausgestaltung von Biobanken zu schaffen. Auf die individuellen Aspekte einer bestimmten Biobank kann daher nicht eingegangen werden. Der hiermit vorgelegte Abschlussbericht der Studie „Rechtliche Ausgestaltung der Datentreuhänderschaft für Biobanken" ist neben dieser Einleitung in sechs weitere Kapitel gegliedert:

Das folgende zweite Kapitel definiert den Begriff der Biobanken sowie deren Besonderheiten und legt damit den Gegenstand der datenschutzrechtlichen Forderungen und Zertifizierung fest. Weiter wird das Spannungsverhältnis zwischen dem Datenschutz (Geberschutz) einerseits und der

Forschungsfreiheit andererseits sowie zwischen den Biobanken und Dritten aufgezeigt. Darauf aufbauend werden die Risiken für das informationelle Selbstbestimmungsrecht dargestellt, die sich nicht nur durch die Verarbeitung bzw. Vorhaltung seiner Daten in Biobanken ergeben, sondern auch durch Interessen Dritter gefährdet werden können. Zuletzt werden die datenschutzrechtlichen Grundlagen des Spenderschutzes sowie der für den Bericht relevanten Input des TP-1 skizziert.

Im dritten Kapitel werden die datenschutzrechtlichen Anforderungen, die für Biobanken zu beachten sind, dargestellt sowie die Datentreuhänderschaft analysiert. Dabei werden die nationalen und internationalen Regelungen zur Datentreuhänderschaft einem Vergleich unterzogen. Ein weiterer Schwerpunkt liegt in der Vorstellung eines Pseudonymisierungsverfahrens, das den Besonderheiten der Biobanken Rechnung trägt.

In dem vierten Kapitel werden weitere notwendige Maßnahmen des Spenderschutzes aufgezeigt, die eine Datentreuhänderschaft flankieren müssen; nämlich die Beschreibung und Festlegung von Prozessen, von verbindlichen (schriftlichen) Arbeitsanweisungen (Standard Operating Procedures – SOPs), von Regeln guter Unternehmensführung (Codes of Conduct) sowie von verbindlichen Transparenzpflichten gegenüber Spendern der Biobank und der Öffentlichkeit.[1]

Kapitel fünf beinhaltet einen internationalen Rechtsvergleich der Auditierungsregeln und stellt Kriterien für eine Auditierung von Biobanken vor.

Das sechste Kapitel fasst die Empfehlungen und Ergebnisse der Studie zusammen.

[1] Die Einschaltung Dritter als spenderschützende Maßnahme wird nicht ausführlich dargestellt.

2 Biobanken und die Risiken für das Recht auf informationelle Selbstbestimmung

2.1 Aktuelle Entwicklungen

Die medizinische Forschung hat in den vergangenen Jahren beträchtliche Fortschritte gemacht, die mit den Stichworten humangenetische Forschung und Biotechnologie bezeichnet werden können. Wesentlichen Anteil hieran haben Großtechniken wie etwa die Hochdurchsatztechnologie, die eine maschinelle Untersuchung von Biomaterial erlaubt, was in kurzer Zeit zu großen und aussagekräftigen Datenmengen führt. Daneben schreitet die Sequenzierung des menschlichen Genoms immer schneller voran, so dass immer mehr Informationen über die genetische Disposition einer Person durch Genanalysen gewonnen werden können.[2] Die Sequenzierung und Kategorisierung der Bausteine des menschlichen Genoms wiederum verspricht ein besseres Verständnis der molekularbiologischen Grundlagen von Krankheiten und wird deren Diagnose zu einem deutlich früheren Zeitpunkt ermöglichen[3]. Die molekulargenetische Diagnostik erlaubt es unter anderem, genetisch bedingte Ursachen oder Veranlagungen zu Krankheiten bereits lange vor Ausbruch der eigentlichen Krankheit zu bestimmen. Diese sog. Gendiagnostik ist derzeit die wichtigste Anwendung der Gentechnologie in der Medizin und reicht von der vorgeburtlichen Diagnostik über den Einsatz in der Gerichtsmedizin bis hin zu Screening-Programmen ganzer Bevölkerungsgruppen[4]. Daneben erfolgt eine vehemente Verbreitung der kommerziellen Nutzung von (prädiktiven) Gentests („Gentests als Lifestyle-Phänomen“). Die Zahl der Unternehmen, die Gentest zu den verschiedensten Zwecken anbietet, steigt stetig an und hat erhebliches Marktpotential[5]. Angeboten werden dem Verbraucher neben Vaterschaft- und Geschwistertests[6] z. B. genetische Test auf Dispositionen für häufig auftretende Krankheiten[7] oder aber den angeblichen Nachweis, in welchem Umfang der Betroffenen vom Zigarettenkonsum abhängig werden kann[8]. Es ist ein ganzer Wissenschafts- und Wirtschaftszweig entstanden, der sich nur um das Erbgut dreht. Daneben werden zum Teil von Arbeitgebern und Versicherungen offen Begehrlichkeiten nach genetischen Untersuchungen geäußert[9].

Parallel zum medizinischen-technischen Fortschritt hat die Quantität und Qualität der Biobanken zugenommen, die sich der fortschreitenden Technik zu bedienen. Hinzu kommt, dass Biobanken in

---

[2] Vgl. z. B. das Human Epigenome Pilot Project, abrufbar unter: http://www.epigenome.org/.
[3] Vgl. Dr. Kurt Berlin, Vorstandsmitglied für Forschung und Entwicklung von Epigenomics, Statement abrufbar unter: http://www.epigenomics.com/pdf_temp/1_Epigenomics_und_das_Wellcome_Trust_Sanger_Institute_starten_Humanes_Epigenomprojekt_HEP_nach_EU-Pilotstudie.pdf.
[4] Forschungsbericht der Interdisziplinäre Arbeitsgruppe der Berlin-Brandenburgische Akademie der Wissenschaften, Gendiagnostik in Deutschland. Status quo und Problemerkundung, Bd. 18, 2007.
[5] Lemke, Allround-Gentest für jedermann, GID 189, August 2008, S. 25-40.
[6] Vgl. z. B. http://www.bj-diagnostik.de/produkte.html.
[7] Z. B. die DNA Direct, Inc. mit Sitz in den USA, die ein Dutzend Test anbietet, die u. a. über die familiäre Krebsdispositonen, Medikamentenunverträglichkeiten oder die Veranlagung für Diabetes aufklären sollen, vgl.: http://www.dnadirect.com/web/article/testing-for-genetic-disorders/.
[8] So die g-Nostics mit Sitz in den UK, die entsprechende DNA-Test anbietet und bewirb: „Differences in our genes mean that some people break down nicotine more quickly than others … We also let you know about another gene that may affect the way your brain reacts to nicotine (DRD2). Some studies suggest that people with different forms of the gene do better with different treatments (bupropion Vs nicotine replacement)”, vgl. unter http://www.g-nostics.com/index.php?option=com_content&task=view&id=7&Itemid=37.
[9] Vgl. Weichert, Der gläserne Mensch – Die Entschlüsselung des menschlichen Genoms als ethische und gesellschaftliche Herausforderung, abrufbar unter: https://www.datenschutzzentrum.de/material/themen/gendatei/genoment.htm#2.

zunehmendem Maße sowohl national als auch international untereinander vernetzt arbeiten, was wiederum die Datenmenge erhöht und eine Standardisierung erforderlich macht.

2.2 Begriffbestimmung und Besonderheiten einer Biobank

2.2.1 Begriffsbestimmung

2.2.1.1 Biobanken

Biobanken sind Sammlungen von Proben menschlicher Körpersubstanzen wie Blut, Gewebe, Zellen und der DNA als Träger genetischer Informationen, die mit personenbezogenen Daten ihrer Spender verknüpft werden beziehungsweise verknüpfbar sind[10]. Zu den in diesem Zusammenhang verknüpften Daten gehören insbesondere Angaben über Krankheiten und Behandlungsverläufe, Medikamenteneinahmen, psychische Dispositionen, familiäre und soziale Situation, Umweltdaten, Verwandtschaftsbeziehungen und Lebensstil. Biobanken haben danach einen Doppelcharakter: Sie umfassen sowohl eine Probensammlung als auch eine Datensammlung,[11] die internen und externen Forschungsprojekten zur Verfügung gestellt werden. Wesentliche Merkmale einer Biobank sind die intendierte oder bereits erfolgte genetische Analyse des Materials sowie dessen langfristige Lagerung[12]. Zum großen Teil dienen die Biobanken der medizinischen und pharmazeutischen Forschung. Eine untergeordnete Rolle spielen Biobanken, die nicht der Forschung dienen und deswegen unberücksichtigt bleiben.

2.2.1.2 Die Datenerhebungsstrukturen bei Biobanken

Man kann man zwischen Biobanken unterscheiden, die ihre Daten direkt bei den Betroffenen erheben und diejenigen, die die Daten indirekt, d. h. aus dem Behandlungszusammenhang gewinnen. Weiter kann man von einer projektbezogenen Proben- und Datenerhebung und einer projektübergreifenden Proben- und Datenerhebung sprechen. Projektbezogene Proben- und Datenerhebung beschaffen dabei Spender für konkrete einzelne Forschungsprojekte. Auch hier besteht im Allgemeinen eine Vorhaltung von Daten und Proben für wechselnde Projekte der Beforschung. Für jedes Projekt gibt es hier aber eine neue (d. h. weitere) Kontaktaufnahme mit dem Spender: Nachdem der Spender seine Einwilligung in die Teilnahme an der Biobank erklärt und dort Proben und Daten abgegeben hat, finden Spenderaufklärung und Spendereinwilligung gesondert für jedes einzelne Forschungsprojekt statt. Der Spender kann deshalb in die Teilnahme an einem Projekt einwilligen, an einem zweiten nicht teilnehmen, sich am dritten wiederum beteiligen. Dieser Folgekontakt kann dabei entweder zwischen dem Forscher und dem Spender[13] oder zwischen der Biobank und dem Spender[14] stattfinden. Bei Biobanken mit projektbezogener Proben- und Datenerhebung haben alle Gesichtspunkte des Spenderschutzes einen Bezugspunkt in einem bestimmten einzelnen Forschungsprojekt.

---

[10] Nationaler Ethikrat, Biobanken für die Forschung, S. 9.
[11] Nationaler Ethikrat, Biobanken für die Forschung, S. 9.
[12] Söns, Biobanken im Spannungsfeld von Persönlichkeitsrecht und Forschungsfreiheit, S. 38.
[13] Dazu zählen etwa diejenigen Biobanken, die geeignete Probanden für die Humanarzneimittelforschung aussuchen. Dies betrifft den hoch regulierten und studienbezogen mit detaillierten Schutzregeln versehenen Bereich der Prüfung von Arzneimitteln und Medizinprodukten, §§ 40 ff. Arzneimittelgesetz (AMG).
[14] So etwa die Biobank des Blutspendedienstes des Bayerischen Roten Kreuzes, vgl. unter http://biobank.blutspendedienst.com/home.html sowie Rapp u. a., Biomarker-Forschung mit einzigartiger Ressource, Laborwelt (Biocom-Verlag), Heft 4/2006, S. 28 ff.

Projektübergreifende Proben- und Datenbankerhebungen zielen dagegen darauf ab, von den Spendern Materialien und Daten von vornherein für wechselnde Projekte der Beforschung einzuwerben. Erneute Spenderkontakte sind nicht angestrebt und finden zwischen Spender und Biobank allenfalls dann statt, wenn die von der Biobank in Aussicht genommenen Zwecke projektübergreifender Beforschung es erfordern, den Spender wiederholt um seine Mitwirkung zu bitten, etwa, um von ihm Daten und Material in Zeitreihen einzuwerben. Kontaktaufnahmen zum Spender mit Rücksicht auf ein einzelnes in Aussicht genommenes Forschungsprojekt finden nicht statt[15]. In der Praxis erfolgt überwiegend eine projektübergreifende Datenerhebung.[16]

2.2.1.3 Personenbezogene/genetische Daten

Personenbezogene Daten sind nach den Datenschutzgesetzen „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)[17]“. Nach § 3 Abs. 9 Bundesdatenschutzgesetz (BDSG) zählen Gesundheitsdaten zu den besonderen Arten personenbezogener Daten (auch sensible Daten genannt), für die spezielle Verarbeitungsregeln gelten[18]. Als „genetische“ Daten werden allgemein diejenigen personenbezogenen Daten bezeichnet, die sich aus dem genetischen menschlichen Material ableiten lassen. Sobald menschliches Material zu Zwecke der Analyse, d. h. zum Extrahieren von Informationen entnommen bzw. vorgehalten werden – wie es bei Biobanken grundsätzlich der Fall ist – bezeichnet man diese als genetische Daten, die ab diesem Zeitpunkt – Personenbezug vorausgesetzt – den Datenschutzgesetzen unterfallen[19]. Diese gelten dagegen nicht für anonymisierte Daten. Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können[20]. Die in der Praxis der medizinischen Forschung vielfach angewandte Methode, den direkten Patientenbezug durch Pseudonyme zu ersetzen, führt nicht zu einer faktischen Anonymisierung im Sinne der Datenschutzgesetze. Bei dieser sog. Pseudonymisierung bleibt eine Zuordnungsfunktion erhalten, mit deren Hilfe der Personenbezug wieder hergestellt werden kann. Pseudonymisierte Daten fallen daher unter den Anwendungsbereich der Datenschutzgesetze[21]. Dies gilt nach hiesiger Auffassung auch dann, wenn die pseudonymisierten Daten von einer Stelle verarbeitet werden, welche selbst nicht über die Zuordnungsfunktion verfügt[22].

---

[15] Beispiele für Biobanken, die als projektübergreifende Vorhaltungsinfrastrukturen geführt werden, sind die Biobanken Popgen (vgl. unter http://www.popgen.de), KORAgen (vgl. unter http://epi.gsf.de/kora-gen/) und die Biobank Indivumed. (vgl. unter http://www.indivumed.com).

[16] Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) zum Entwurf der Bundestagsfraktion Bündnis 90/Die Grünen eines Gendiagnostikgesetzes vom 3.11.2006 (BT-Drs. 16/3233) zur Anhörung am 7.11.2007, abrufbar unter https://www.datenschutzzentrum.de/medizin/genom/20071107-gendiagnostikgesetz.pdf; siehe auch unter Textziffer 2.6 Empirischer Input TP-1.

[17] § 3 BDSG.

[18] Vgl. §§ 13 Abs. 2, 14 Abs. 5, 28 Abs. 6-9, 29 Abs. 5 BDSG.

[19] Vgl. Dammann, in Simitis (Hrsg.), Bundesdatenschutzgesetz, 6. Auflage 2006, § 3 Rn. 5:

[20] § 3 Abs. 6 BDSG.

[21] Weichert, in Däubler et al., Bundesdatenschutzgesetz – Basiskommentar, 2. Auflage 2007, § 3 Rn. 45 ff. So auch die Art. 29-Datenschutzgruppe, WP 136, Stellungnahme Nr. 4/2007 zum Begriff der personenbezogenen Daten, S.18:

[22] Diese Auffassung ist allerdings nicht unbestritten. Vgl. Dammann, in Simitis (Hrsg.), Bundesdatenschutzgesetz, 6. Auflage 2006, § 3 Rn. 35: Für den Empfänger von pseudonymisierten Daten liegen dann keine personenbezogenen Daten vor, wenn ihm die Zuordnungsfunktion (von Pseudonym zu natürlicher Person) nicht zugänglich ist. In diesem Sinne für das Parallelproblem des Personenbezugs von IP-Adressen in Logfiles von Webservern auch AG München, Urt. vom 30.9.2008,

2.2.2 Besonderheiten einer Biobank

2.2.2.1 Sammlung und Vorhaltung von genetischem Material

Die datenschutzrechtlichen Besonderheiten einer Biobank ergeben sich zunächst aus der Tatsache, dass genetische Informationen zur genetischen Analyse gesammelt und vorgehalten werden. Genetische Daten sind allerdings von besonderer Qualität und können die Persönlichkeitsrechte der Betroffenen in besonderem Maße berühren.

Zunächst lassen sich aus allen Körperzellen in kleinsten Mengen genetische Informationen gewinnen. Genetische Daten lassen sich daher ohne Schwierigkeiten beschaffen[23]. Entsprechende Proben können jahrelang aufbewahrt und jederzeit zur Informationsgewinnung verwendet werden. Gendaten sind daher fast uneingeschränkt verfügbar und können darüber hinaus ohne und gegen den Willen des Betroffenen gewonnen werden.

Weiter ist die Qualität der genetischen Information eine besondere: Eine genetische Analyse kann eine genetische Disposition für eine bestimmte Krankheit oder andere genetische Defekte offenbaren, lange bevor diese tatsächlich auftreten. Es handelt sich daher um für den Einzelnen u. U. sehr belastende Informationen über seine Zukunft. Dies gilt insbesondere, wenn für die prognostizierte Krankheit keine oder wenige Therapiemöglichkeiten bestehen. Genetische Dispositionen sind überdies irreversibel und behalten ihre Voraussagekraft für das ganze Leben. Der Mensch ist durch diese Information für sein ganzes Leben beeinflusst.

Hinzu kommt, dass die genetischen Untersuchungen den Gesunden lediglich über die Wahrscheinlichkeit, in der Zukunft zu erkranken, informiert, ohne dass der zeitliche Rahmen oder das tatsächliche Eintreten konkret bestimmbar ist. Von wenigen Ausnahmen[24] abgesehen ist dabei nicht sicher, dass sich die prognostizierte Tatsache bewahrheitet. Die Information kann den Betroffenen daher völlig unnötig belasten bzw. die Zeit vor Ausbruch der Krankheit erschweren.

Ein weiterer Faktor ist die Nicht-Vorhersehbarkeit der gewinnbaren Informationen. Ein Teil der in einer Biobank aufgenommener Daten wird erst durch zukünftige Forschungen und den allgemeinen Fortschritt der Wissenschaft nach und nach erschlossen. Selbst wenn der Betroffene bereit ist, bestimmte genetische Informationen, die aus der Analyse seiner Gene gewonnen werden, zu erhalten oder seine Daten für die Forschung zur Verfügung zu stellen, so ist fraglich, ob er auch die zukünftig gewinnbaren Informationen erhalten möchte, deren Erfassbarkeit zum jetzigen Zeitpunkt nicht konkret absehbar ist. Gibt der Betroffene daher sein Erbgut für die Forschung frei, besteht die Möglichkeit, dass angesichts der Forschungsentwicklung eine für ihn nicht überschaubare Anzahl an Informationen verfügbar werden, die ihm vielleicht nicht bekannt werden, aber die damit jedenfalls in der Welt sind. Hinzu kommt, dass personifizierte Gewebeproben nicht nur für einen bestimmten Zweck nach einer

---

K&R 2008, 767 mit zustimmender Anmerkung von Eckhardt. Mit Einschränkungen folgen dieser Ansicht namentlich für den Bereich der medizinischen Forschung Arning/Forgó/Krügel, Datenschutzrechtliche Aspekte der Forschung mit genetischen Daten, DuD 2006, 700, 705.

[23] Artikel 29-Datenschutzgruppe, WP 91, Arbeitspapier über genetische Daten, S. 5.

[24] Wie Chorea Huntington.

bestimmten Analysemethode ausgewertet werden können, sondern praktisch zur Beantwortung jeder genetisch beantwortbaren Fragestellung geeignet sind. Gendaten beinhalten daher ein Risiko, dessen Beherrschbarkeit durch den Einzelnen ganz überwiegend fehlt.

Schließlich ist auch zu bedenken, dass genetische Informationen gleichzeitig genetische Dispositionen für Blutsverwandte oder zukünftige Nachkommen aufzeigen können und damit auch Dritte betroffen sind.

Zuletzt lassen sich mit genetischen Informationen Personen identifizieren oder Bezüge zwischen Verwandten[25] oder die Zugehörigkeit zu bestimmten Gruppen herstellen oder überprüfen. Weiterhin lassen sich physische Merkmale erkennen, die nicht als Gesundheitsdaten zu klassifizieren sind. Sie sind aber geeignet, z. B. die ethnische Herkunft einer Person zu ermitteln und bergen damit die Gefahr einer entsprechenden Diskriminierung[26].

Insgesamt ergibt sich eine fundamentale Bedeutung der genetischen Information für den Einzelnen.

2.2.2.2 Nicht-Anonymisierbarkeit von genetischen Daten

Eine Besonderheit genetischer Analysen von Gewebeproben besteht darin, dass es praktisch keine Möglichkeit einer sicheren Anonymisierung gibt. Durch identifizierte Referenzgewebeproben oder Ergebnisse aus anderen Genom-Analysen lässt sich jede Probe einer bestimmten Person oder einer verwandtschaftlich nahe stehenden Person eindeutig wieder zuordnen, auch wenn ansonsten keine Angaben über die betroffene Person bekannt sind. Auch ist in der Forschung eine Anonymisierung der Daten nicht immer gewollt ist, da der Forschungszweck ansonsten gefährdet würde[27]. Die Forschungsprojekte bedürfen häufig der wiederholten Ansprache derselben Spenderinnen und Spender, um Gesundheitsinformationen in Zeitreihen zu gewinnen. Die zu unterschiedlicher Zeit zu derselben Person gewonnenen Informationen müssen einander zugeordnet werden können. Zuletzt lassen sich bei fortschreitender Technik immer mehr Informationen aus dem genetischen Material gewinnen, so dass die Gefahr eine Re-Identifizierung durch die zusätzlich gewonnenen Daten besteht.

2.2.2.3 Weitere Besonderheiten einer Biobanken

Biobanken haben grundsätzlich die Tendenz, möglichst viele Daten zu sammeln und sich zu vernetzen, um Erfolge z. B. bei der Erforschung seltener Krankheiten erzielen zu können. Der Datenumfang und die Datenmenge einer Biobank steigen mit der kontinuierlichen Beforschung und dem laufenden Fortschritt der Technik im Laufe der Zeit stetig an. Die Zweckbestimmung ist bei der Erhebung der Daten im Regelfall weit gefasst, da Proben und Daten grundsätzlich für eine Vielzahl von Forschungsprojekten verwendet werden sollen. Es sollen nahezu unbegrenzte medizinische Fragestellungen durch die verschiedensten Stellen, die auch im Ausland liegen können, beantwortet

---

[25] Siehe z. B. Motluk, Anonymous sperm donor traced on internet (3. November 2005) New Scientist (vgl. unter http://www.newscientist.com/article.ns?id=mg18825244.200).
[26] Artikel 29-Datenschutzgruppe, WP 91, Arbeitspapier über genetische Daten, S. 6.
[27] Luttenberger, Reischl, Schröder, Stürzebecher, Datenschutz in der pharmakogenetischen Forschung – eine Fallstudie, DuD 2004, 356, 357.

werden. Zuletzt zielt die Vorhaltung der Proben und Daten in einer Biobank grundsätzlich auf eine möglichst langfristige Dauer.

Die besondere Schutzbedürftigkeit von genetischen Daten, die Unmöglichkeit einer absoluten Anonymisierung der Daten sowie die Vorhaltung einer großen Menge von Daten zu möglichst offenen Zwecken mit langen Aufbewahrungsdauer verlangen nach besonderen Regeln und Maßnahmen zum Schutz der Spender.

2.3 Spannungsverhältnis Spenderschutz/Datenschutz – Forschungsfreiheit

Forscher, die in dem Medizinbereich bzw. in der Genetik forschen, benötigen dazu eine Vielzahl von (genetischen) Daten, um zu einem validen Ergebnis zu gelangen. Art. 5 Abs. 3 Grundgesetz (GG) bestimmt, das die Wissenschaft, d. h. Forschung und Lehre, frei ist. Der Staat ist verpflichtet, diese Freiheitsgarantie zu schützen und zu fördern[28], ohne dass für den Forscher ein verfassungsunmittelbares Datenzugangsrecht besteht.[29] Benötigt die Forschung personenbezogene Daten, so tangiert dies das informationelle Selbstbestimmungsrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG der Personen, die ihre Daten für die Forschung zur Verfügung stellen. Es stehen damit zwei Grundrechte nebeneinander: das Grundrecht auf Wissenschaftsfreiheit und das Grundrecht auf informationelle Selbstbestimmung. Beide Grundrechte sind von existentieller Bedeutung für die Gemeinschaft und den Einzelnen. Zwischen diesen beiden Rechtspositionen ist der Ausgleich durch praktische Konkordanz zu suchen.

Der Gesetzgeber hat für diesen Ausgleich bisher die allgemeinen und die bereichsspezifischen Datenschutzregelungen mit ihren Forschungsklauseln erlassen. Daneben bestehen einige bereichsspezifische Regelungen in einigen Landeskrankenhausgesetzen bzw. Gesundheits- und Krankenhausdatenschutzgesetzen. Weiter sind Forschungsklauseln z. B. in Statistikgesetzen, in Archivgesetzen und in den Sozialgesetzbüchern enthalten. Eine gesetzgeberische Regelung für Biobanken ist bisher nicht erlassen worden. Die geltenden Datenschutzgesetze gehen von einem Verbot mit Erlaubnisvorbehalt aus. Danach ist für die Zulässigkeit der Datenverarbeitung die Einwilligung des Betroffenen erforderlich, es sei denn, eine gesetzliche Regelung bestimmt im überwiegenden Interesse der Allgemeinheit anderes. Damit ist Datenerhebung und –verarbeitung in der Biobank-Forschung nur auf freiwilliger Basis, d. h. auf der Grundlage einer Einwilligung möglich (weitere Einzelheiten dazu unter der 2.6).

2.4 Risiken für den Spender

Biobanken beherbergen eine Vielzahl von Risiken für den Spender, die sich insbesondere aus den oben dargestellten Besonderheiten ergeben.

---

[28] Jarass/Pieroth, Grundgesetz, 9. Auflage, Art. 5 Rn. 101.
[29] Bizer, Forschungsfreiheit und Informationelle Selbstbestimmung, S. 90 f.

2.4.1 Das Risiko einer unfreiwilligen und unbestimmten Einwilligung

2.4.1.1 Freiwilligkeit der Spende

Eine Spende für die Biobank-Forschung ist nur auf freiwilliger Basis denkbar. Ob die Zurverfügungstellung von Proben freiwillig, das heißt frei von jedem (inneren oder äußeren) Zwang, abgegeben wird bzw. abgegeben werden kann, ist zweifelhaft. Dieses Problem stellte sich insbesondere bei einer Proben- und Datenerhebung im Zusammenhang mit einer medizinischen Behandlung. Die Betroffenen können in ihrer freien Entscheidung beeinträchtigt sein, weil sie fürchten, dass ihnen andernfalls nicht die optimale Behandlung angedient wird. Zudem erschwert die in diesen Fällen hinzukommende ärztliche „Autorität“ die freie Entscheidungsmöglichkeit des Betroffenen. Hinzu kommt, dass der Betroffene, der als Patient in die Erhebung und Verarbeitung seiner Proben und Daten einwilligt, unter Umständen nicht in der gesundheitlichen Verfassung ist, sich Zeit für eine freie Entscheidung zu nehmen.

2.4.1.2 Bestimmtheit der Einwilligung und Informiertheit des Spenders

Es besteht das Risiko, dass der Zweck der Forschung, die Speicherdauer, die potentiellen Empfänger der Daten, der für die Datenverarbeitung Verantwortliche sowie die allgemeinen Risiken der genetischen Analyse für den Spender in dem Moment seiner Einwilligung nicht hinreichend erkennbar gemacht werden und dieser dadurch keine (wirksame) Einwilligung treffen kann. Gemäß dem von den meisten Biobanken verfolgten Ziel, die Proben und Daten für möglichst viele Forschungsprojekt zur Verfügung zu stellen, besteht die Gefahr, dass der Spender nicht überblickt, für welches Forschungsprojekt er sein Einverständnis erteilt hat bzw. nur die Möglichkeit hat, pauschal in die Verwendung seiner Daten zu Forschungszwecken einzuwilligen. Er willigt dann in Forschungsprojekte der Zukunft ein, deren Inhalte und technische Voraussetzungen noch gar nicht feststehen. In diesem Zusammenhang steht die möglichst langfristige Aufbewahrung und Nutzung der Proben. Je länger die Proben vorgehalten werden, desto größer das Risiko, dass der Spender das Wissen und die Herrschaft über seine Daten verliert. Eine unbegrenzte Speicherung birgt auch im Hinblick auf die zukünftigen technischen Entwicklungen die Gefahr, dass eine Abschätzung der Risiken, die mit der genetischen Forschung einhergehen, für den Einzelnen nicht mehr einsehbar ist. Gleichermaßen fehlen ihm dann Informationen über die Empfänger seiner Daten und die Verantwortlichen der Datenverarbeitung.

Ausgleichend muss dem Spender für den Fall der beabsichtigten genetischen Beforschung die Konsequenzen seines Einverständnisses besonders verdeutlicht werden. Ohne diese Informationen kann der Spender weder sein Auskunfts-, noch sein Widerrufs-, noch sein Löschungsrecht geltend machen. Es besteht das Risiko, dass die Betroffenen ihr informationelles Selbstbestimmungsrecht nicht ausüben können.

2.4.2 Das Risiko der Belastung des Spenders mit unerwünschtem Wissen

Das Wissen um eine Diagnose bzw. das Wissen um das Risiko einer künftigen Erkrankung (das auch die Chance ihres Nichteintritts einschließt), kann für den Spender eine erhebliche Belastung bedeuten. Neben dem Recht, über die Erhebung, Verwendung und Nutzung der eigenen Daten und damit über die Kenntnisnahme seiner Daten durch Dritte selbst zu bestimmen, hat der Betroffenen auch ein

schützenswertes Interesse daran, selbst von dem Wissen über seine genetische Veranlagung verschont zu bleiben. Es ist anerkannt, dass das Recht auf Nichtwissen eine Konkretisierung des Rechts auf informationelle Selbstbestimmung ist und entsprechendem Schutz genießt[30].

2.4.3 Das Risiko des Bruchs der Vertraulichkeit

Jede personenbezogene Datensammlung beinhaltet das Risiko eines Vertrauensbruchs. Die Vertraulichkeit kann dabei sowohl durch interne als auch durch externe Angriffe verletzt werden. Besondere Bedeutung erlangt der Schutz der Vertraulichkeit im Rahmen der Biobankenforschung, weil die Auswirkungen einer unbefugten Offenbarung besonders nachhaltig sind, sehr schwerwiegend und neben dem Biobankspender auch andere Personen betreffen können. Es ist daher eine wesentliche Aufgabe einer Biobank, dieses Risiko zu beherrschen.

Biobanken, die Proben und Daten der Spender bei Hereinnahme anonymisieren, müssen ein geringeres Risiko beherrschen und verantworten, als Biobanken, die dies erst bei der Herausgabe der Daten an einzelne Forschungsprojekte tun. Noch größere Risiken für die Vertraulichkeit gehen Biobanken ein, die die Daten mit einem Spenderpseudonym versehen herausgeben. Das Risiko ist klein, wenn das Pseudonym auf das Forschungsprojekt bezogen ist. Noch kleiner ist es, wenn es sich bei dem Pseudonym um ein Einwegpseudonym handelt. Weiter ist das Risiko von der Vernetzung der Biobanken bzw. von der Durchführung von gemeinsamen oder externen Forschungsvorhaben abhängig. Eine wesentliche Rolle kommt deshalb der Vorhaltung von Daten und Proben bei der Biobank und dabei dem Umgang der Biobank mit den Daten zu, die den Spender identifizieren.

2.4.4 Das Risiko der unzulänglichen Anonymisierung/Pseudonymisierung

Zu der Tatsache, dass genetische Daten nicht in absoluter Weise anonymisiert werden können und die Forschung eine solche Anonymisierung vielfach auch nicht wünscht, kommt hinzu, dass die Forschungen Ergebnisse zu Tage fördern können, die für den Spender von wesentlicher gesundheitlicher Bedeutung sind. Dort, wo neben einer wiederholten Spenderbefragung eine entsprechende Rückmeldung hierüber an den Spender sachlich angezeigt und rechtlich geboten ist, darf keine irreversible Anonymisierung vorgenommen werden.

2.4.5 Das Risiko tatsächlich nicht durchsetzbarer Spenderrechte

Bei einer fortschreitenden Vernetzung der Biobanken und Erhebung der Daten für offene Zwecke bei langer Speicherdauer wird es für Betroffenen zunehmend schwerer bis unmöglich, die Ansprechpartner für ihre datenschutzrechtlichen Auskunftsansprüche zu identifizieren und so ihr informationelles Selbstbestimmungsrecht wahrzunehmen.

2.5 Interessen Dritter

2.5.1 Arbeitgeber / Versicherungen

Arbeitgeber können unter Umständen ein Interesse daran haben, genetische Informationen über ihre Arbeitnehmer zu erhalten. Sie können z. B. zu erfahren suchen, ob diese eine Veranlagung für

[30] Weichert, Der Schutz genetischer Daten, DuD 2002, 133, 134.

bestimmte Krankheiten haben und für den Arbeitsplatz ungeeignet sein könnten. Auch Informationen über Eigenschaften und Charakter des Arbeitnehmers könnten zukünftig gewonnen werden und von Interesse sein. Ein direkter Zugriff des Arbeitgebers auf Informationen aus einer Biobank ist unwahrscheinlich, es ist aber zu bedenken, dass das systematische Vorhalten von genetischen und medizinischen Daten in Biobanken dazu führen kann, Begehrlichkeiten bei den Arbeitgebern zu wecken und entsprechende Forderungen an den Arbeitnehmer zu stellen. Je höher die Verfügbarkeit und je umfassender die Katalogisierung von genetischen Daten ist, desto größer wird der Druck, diese auch für andere Zwecke als die Forschung zu nutzen. Dabei muss der Druck nicht direkt vom Arbeitgeber ausgeübt werden. Denn es genügt, dass ein anderer seine Geeignetheit freiwillig durch Vorlage eines Gentestes nachweist, der über eine günstige Disposition verfügt und damit den Konkurrenten indirekt zum Offenbaren auffordert. Hinzu kommt, dass der Betroffene selbst eventuell noch gar keine Kenntnis von seiner genetischen Disposition hat und auch nicht haben will, sondern vielmehr von seinem Recht auf Nichtwissen Gebrauch machen möchte.

Entsprechendes gilt für die Versicherungsbranche. Private Versicherungen übernehmen Risiken, die die Gesundheit und die Lebensführung der Person betreffen. Die Versicherungsprämie richtet sich nach der Wahrscheinlichkeit des Eintritts des „Schadenfalles“. Insoweit ist es für die Kalkulation des Risikos für den Versicherer von erheblicher Bedeutung, Informationen über Krankheitsveranlagungen und ähnliches sowie über die Lebensführung des Versicherten zu erhalten, um so sein Versicherungsrisiko präziser bewerten zu können. Genetische Informationen würden damit die Konditionen für den Einzelnen erheblich beeinflussen. Es besteht gleichermaßen die Gefahr der Zweckentfremdung der Forschungsdaten durch indirekten Druck wie im Arbeitsbereich.

2.5.2 Strafverfolgungsbehörden

Biobanken können, da sie große Datenbestände über einen großen Teil der Bevölkerung enthalten bzw. aufbauen, die Begehrlichkeiten von Strafverfolgungsbehörden wecken. Diese können mittels ihrer Befugnisse unter bestimmten Voraussetzungen die Beschlagnahme von in Biobanken enthaltenen Daten bewirken. Eine Beschlagnahme bzw. eine Auswertung der Daten und Proben ist nur dann nicht möglich, wenn Daten einem Arzt anvertraut sind, §§ 53 Abs. 1, 95 StPO. Diese Voraussetzung liegt jedoch bei der Vorhaltung von Proben und Daten in einer Biobank in der Regel nicht vor. Damit ist in bestimmten Fällen ein Zugriff der Strafverfolgungsbehörden möglich.

2.6 Rechtliche Grundlagen der Risikobewältigung

Die Daten- und Probensammlung und -vorhaltung zum Zwecke der Forschung in Biobanken betrifft neben allgemeinen Fragen des Arztrechtes, Eigentumsrechts und Strafrechts insbesondere Fragen des Persönlichkeitsrechts und des Datenschutzes, der im Fokus des Berichtes steht. Die Verwendung von Proben und Daten fällt unter den Anwendungsbereich der Datenschutzgesetze. Diese erstrecken ihren Schutz auf jede Information über eine natürliche Person und umfassen auch die Proben, sobald diese – wie stets in Biobanken – zum Zwecke der Analyse vorgehalten werden. Bei beruflicher ärztlicher Tätigkeit findet das Standesrecht und der strafrechtliche Schutz der ärztlichen Schweigepflicht nach § 203 StGB Anwendung.

Zurzeit besteht mit dem kürzlich vom Bundestag verabschiedeten Gendiagnostikgesetz eine gesetzliche Grundlage ausschließlich für genetische Untersuchungen und im Rahmen genetischer Untersuchungen durchgeführte genetische Analysen und den Umgang mit dabei gewonnenen genetischen Proben und Daten bei genetischen Untersuchungen zu medizinischen Zwecken, zur Klärung der Abstammung sowie im Versicherungsbereich und im Arbeitsleben. Das Gesetz gilt nicht für genetische Untersuchungen und Analysen und den Umgang mit genetische Proben und Daten zu Forschungszwecken.[31] Es fehlt daher an einem, speziell für die Biobank-Forschung geltenden Gesetz.[32] Mangels entsprechender gesetzlicher Regelung ist in jedem Fall für die Biobank-Forschung die Einwilligung der Betroffenen erforderlich. Dies gilt auch für die Proben, die ursprünglich für eine ärztliche Behandlung erhoben worden sind. Diese Proben können so lange aufbewahrt werden, wie es für die Durchführung der Behandlung erforderlich ist. Eine spezielle gesonderte Einwilligung ist hierfür nicht erforderlich. Eine systematische langfristige Aufbewahrung der Proben, wie sie grundsätzlich in Biobanken vorgesehen ist, ist damit jedoch nicht gedeckt. Eine entsprechende gesetzliche Ermächtigung lässt sich auch nicht den Landesdatenschutzgesetzen oder den Landeskrankenhausgesetzen entnehmen (mit der Ausnahme von Hamburg, dessen landesrechtliche Regelung ausdrücklich krankhausinterne Biobanken umfasst). Teilweise enthalten diese Gesetze zwar Regelungen über die Möglichkeit der Durchführung von Forschungsvorhaben ohne Einwilligung der Betroffenen. Diese beziehen sich jedoch grundsätzlich auf konkrete Forschungsvorhaben. Eine Rechtsgrundlage für die Aufbewahrung und Sammlung von Proben und Daten in einer Biobank, die eine langfristige Aufbewahrung und Verwendung für eine unbestimmte Mehrheit von Forschungsprojekten vorsieht, ist damit nicht gegeben.

Zu den allgemeinen Wirksamkeitsvoraussetzungen einer datenschutzrechtlichen Einwilligung („informed consent“, vgl. § 4a BDSG) müssen weitere Zulässigkeitsbedingungen bestehen, um den Betroffenen vor Zwangslagen und unbedachten existenziellen Erklärungen zu schützen. Diese werden unter 3.4 ff. näher dargestellt.

2.7 Empirischer Input TP-1

Die Analyse und Klassifikation der Biobanken durch TP-1 hat – auszugsweise und kurz gefasst – die folgenden Ergebnisse ergeben, die von TP-2 berücksichtigt worden sind bzw. die die Notwendigkeit der Verbesserung des Spenderschutzes durch neue Treuhandmodelle, Selbstregulierung, Transparenzpflichten und Auditierung belegen[33]:

- Jede Biobank hat eigene „Prozess-Signatur“, d. h. jede Biobank hat unterschiedliche betriebliche Prozesse festgelegt, es gibt keine Standardvorgaben,
- Eine Trennung von Verantwortlichkeiten ist nicht konsequent durchgeführt,

[31] Vgl. auch Fußnote 172.

[32] Datenschutzrecht ist im privaten Bereich nur anwendbar, wenn eine Datenverarbeitung in oder aus einer Datei oder durch Datenverarbeitungsanlagen erfolgt (§ 1 Abs. 2 Nr. 3 BDSG, vgl. § 27 Abs. 1 BDSG). Es entspricht sowohl dem Sinn wie auch dem Wortlaut des Gesetzes, in der Genanalyse eine Nutzung von Daten durch eine Datenverarbeitungsanlage zu sehen. Auf das Vorliegen des Dateibegriffs kommt es damit nicht an. Genetische Daten sind in jedem Fall „aus einer automatisierten Verarbeitung entnommen“ (§ 27 Abs. 2 BDSG).

[33] Die Ergebnisse der Studie sind in dem interdisziplinären Workshop „Datenschutzrechtliche Auditierung von Biobanken“ in Kiel am 4. Juli 2008 vorgestellt worden. Die dargestellten Feststellungen sind unter http://www.datenschutzzentrum.de/biobank/kollek-paslack-2008-empirie-analyse-biobank.pdf. nachlesbar.

- Hinsichtlich des Pseudonymisierungsverfahrens besteht fast überall – z.T. sogar erheblicher – Nachbesserungsbedarf,
- Formalisierte Materialtransfervereinbarungen mit den Empfängern von Daten/Proben fehlen,
- Es erfolgen keine effektiven Kontrollen der Empfänger,
- Eine mögliche Rückmeldung relevanter Forschungsergebnisse wird sehr unterschiedlich gehandhabt,
- Biobanken reagieren unterschiedlich auf Spenderwiderrufe,
- Die Spenderinformationen enthalten zum Teil keine oder nicht ausreichende Angaben über:
    - die Eingriffstiefe (genetische Untersuchungen),
    - die Teilnahme an zukünftigen Projekten,
    - das Verfahren nach Widerruf,
    - die Voraussetzungen und das Verfahren für eine erneute Kontaktaufnahme,
    - die Pseudonymisierung / Anonymisierung der Daten,
    - den Zugriff auf die Daten,
    - Daten- und Probenübermittlungen an Dritte,
    - den Verbleib der Daten bzw. Proben nach Ausscheiden aus der Studie,
    - die Eigentumsverhältnisse an der Probe,
    - die Risiken der Teilnahme,
    - Kontaktadressen /Ansprechpartner für die Ausübung von Spenderrechten.
- Die Spendereinwilligungen enthalten zum Teil keine oder nicht ausreichende Angaben über
    - den Titel der Studie / der Biobank,
    - eine Bestätigung der Aufklärung durch den Arzt,
    - Wahlmöglichkeiten für / gegen Erhebung bestimmter Daten,
    - die implizierte Zustimmung zu anderen Studien,
    - Wahlmöglichkeiten für / gegen Teilnahme an zukünftigen Forschungsprojekten,

  bzw. ist die Verarbeitungseinwilligung nicht als gesonderte Erklärung erkennbar.

3 Allgemeine Datenschutzrechtliche Anforderungen

Die Biobank-Forschung ist nur verantwortbar, wenn die Spenderdaten umfassend geschützt sind.

3.1 Rechtsgrundlagen des Spenderschutzes

Rechtsgrundlage des Spenderschutzes sind die Eigentumsrechte, die sog. Spenderautonomie und das Recht auf informationelle Selbstbestimmung. Die ersteren Rechtsgrundlagen sollen nur kurz skizziert werden, da der Schwerpunkt des Berichts auf dem Recht auf informationelle Selbstbestimmung liegt.

3.1.1 Eigentumsrecht

Die Verarbeitung von Proben wirft Eigentumsfragen auf, da das Verbrauchen der Proben im Rahmen der Forschung genau genommen nur zulässig ist, wenn die Probe sich im Eigentum der Forschung befindet d. h. der Spender das Eigentum übertragen hat[34]. Eine Anonymisierung stellt ohne Eigentumsübertragung eine Pflichtverletzung dar, da der Bezug zum Eigentum des Spenders damit aufgehoben wird[35]. Andererseits ist fraglich, ob eine Eigentumsübertragung möglich ist bei gleichzeitiger Einräumung eines datenschutzrechtlich gebotenen Widerrufsrechts. Insoweit sind zugleich eigentumsrechtliche Fragen zu klären, die die Rechtsstellung des Spenders betreffen, die jedoch nicht Gegenstand des Berichts sein sollen.

3.1.2 Spenderautonomie

Das Recht auf informationelle Selbstbestimmung ist eine von mehreren – vom Bundesverfassungsgericht herausgearbeiteten – Ausprägungen des Persönlichkeitsrechts, das grundrechtlich gem. Art 2 Abs. 1 i. V. m. Art 1 Abs. 1 GG geschützt ist.[36] Sie bezieht sich auf die Selbstbestimmung hinsichtlich personenbezogener Informationen.

Daneben bildet die sog. Spenderautonomie[37] eine weitere – neue – Ausprägung des allgemeinen Persönlichkeitsschutzes. Diese garantiert das Recht, grundlegende Fragen der eigenen Lebensführung eigenständig treffen zu können und im Einklang mit der gewählten Konzeption zu leben. Dieses Recht enthält zunächst die Autonomie bezüglich der Entscheidung über Teilnahme, Eingliederung und Analyse von Gewebematerialien in Biobanken sowie die Befugnis, über die Dispositionen der eigenen Erbanlage Kenntnis zu erlangen oder in Unkenntnis zu bleiben. Umfasst von diesem Schutz sind auch anonymisierte genetische Daten. Da eine absolute Anonymisierung von genetischen Daten nicht möglich ist und jedenfalls in nicht allzu ferner Zukunft aufgrund der fortschreitenden Analysemethoden und -techniken von einem ausreichenden Grad der Anonymisierung nicht mehr ausgegangen werden kann, unterfallen diese Daten aufgrund ihres herstellbaren Personenbezuges auch dem Recht auf informationelle Selbstbestimmung, so dass die Spenderautonomie im Wesentlichen von dem Recht auf informationelle Selbstbestimmung mit umfasst wird.

---

[34] Artikel 29-Datenschutzgruppe, WP 91, Arbeitspapier über genetische Daten, S. 9.
[35] TMF, Ein generisches Datenschutzkonzept für Biomaterialbanken, Version 1.0, April 2006, S. 21.
[36] Söns, Biobanken im Spannungsfeld von Persönlichkeitsrecht und Forschungsfreiheit, S. 79ff.
[37] Söns, Biobanken im Spannungsfeld von Persönlichkeitsrecht und Forschungsfreiheit, S. 108.

3.1.3 Datenschutzrecht: Allgemeine Datenschutzrechtliche Forderungen

Das informationelle Selbstbestimmungsrecht beinhaltet grundsätzlich das Recht des Einzelnen, selbst den Inhalt der Informationen und den Kommunikationspartner festzulegen und damit selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.[38] Geschützt sind alle Daten, unabhängig von ihrer Art und Bedeutung für den Einzelnen, da es aufgrund der neuen Möglichkeiten der Verknüpfungen mit anderen Daten und Sachverhalten kein belangloses Daten mehr gibt. [39] Im letzten Jahr hat das Bundesverfassungsgericht als wiederum neue Ausprägung des allgemeinen Persönlichkeitsrechts festgestellt, dass dieses Grundrecht auch die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. Es hat die Verantwortung des Staates für biotechnologische Datenverarbeitung und die Erforderlichkeit des Schutzes durch Verfahren und Technik hervorgehoben.[40]

3.1.3.1 Erlaubnis, Rechtmäßigkeit und Nutzung

Jede Verarbeitung personenbezogener Daten bedarf einer gesetzlichen Grundlage oder der Einwilligung des Betroffenen (sog. Erlaubnisvorbehalt). Die Erhebung und Verarbeitung von personenbezogenen Daten in Biobanken ist, wie dargestellt, nur mit Einwilligung des Betroffenen zulässig.

3.1.3.2 Einwilligung

Jede Einwilligung muss freiwillig, bestimmt und informiert erfolgen[41]. Sie ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Dies bedeutet, dass weder indirekter noch direkter Druck auf die Spender ausgeübt werden darf. Folge der Freiwilligkeit ist, dass der Betroffene die Einwilligung jederzeit widerrufen kann. Die Einwilligung muss in allen Punkten (wer übermittelt wann was an wen zu welchem Zweck) so bestimmt sein, dass für ihn eindeutig erkennbar ist, was mit seinen Daten geschieht. Nur wer das überblickt, ist hinreichend informiert, um wirksam einwilligen zu können. Es ist auf

- den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie
- den geplanten Umfang der Datenverarbeitung
- den Personenkreis, der von den personenbezogenen oder anonymisierten Daten Kenntnis erhält
- den Zeitpunkt der Löschung
- die Verantwortlichen
- die Folgen der Verweigerung der Einwilligung hinzuweisen.

Ist die Information so gestaltet, dass sie bei einem durchschnittlichen Betroffenen zu falschen Vorstellungen über die Art, den Umfang und den Zweck sowie die verantwortliche Stelle führen muss, so ist sie nicht freiwillig oder nicht ausreichend bestimmt. Die auf der Grundlage einer solchen Information abgegebene Einwilligung ist unwirksam und damit die Datenverarbeitung rechtswidrig.

---

[38] BVerfGE 65,1, 42, 78, 84 (Volkszählungsurteil).
[39] BVerfGE 65,1, 45 (Volkszählungsurteil).
[40] Vgl BVerfGE vom 27. Februar 2008 – 1 BvR 370/07; 1 BvR 595/07.
[41] Vgl. § 4a Abs. 1 Satz 1 BDSG.

3.1.3.3 Zweckbindung

Personenbezogene Daten dürfen nur zu dem Zweck verarbeitet und genutzt werden, zu dem sie erhoben worden sind. Diese Zweckbindung ist ein wesentliches Grundprinzip des Datenschutzrechts. Der Betroffene soll wissen und entscheiden, zu welchen Zwecken seine Daten verarbeitet werden.

3.1.3.4 Erforderlichkeit und Datensparsamkeit

Die Verarbeitung von personenbezogenen Daten ist nach Art, Umfang und Dauer nur in den Grenzen der Erforderlichkeit zulässig. Die verantwortliche Stelle darf nur so viele personenbezogene Daten verarbeiten, wie es nach der mit dem Betroffenen getroffenen Vereinbarung (Einwilligung) bzw. nach dem Gesetz erforderlich ist. Fehlt die Erforderlichkeit, sind die Daten zu löschen. Die technische Seite der Regel der Erforderlichkeit ist das Gebot der Datensparsamkeit. Die Regeln zur Datenvermeidung bzw. Datensparsamkeit sind vor allem als Gestaltungsanforderungen für IT-Systeme und elektronische Datenverarbeitungsvorgänge zu verstehen. Ziel ist es, keine oder möglichst wenige personenbezogene Daten anfallen zu lassen. Eine der möglichen Maßnahmen ist die frühestmögliche Kappung des Personenbezugs durch Anonymisierungs- oder Pseudonymisierungsverfahren.

Grundsätzlich ist in der Forschung eine frühestmögliche Pseudonymisierung und Anonymisierung sowie der Zeitpunkt der Löschung vorzusehen. Dafür sind Lösch- und Prüffristen vorzusehen.

3.1.3.5 Transparenz und Betroffenenrechte

Die Transparenz der Datenverarbeitung erfordert, dass der Betroffene über die Daten verarbeitende Stelle, die Verwendungszwecke und die Kategorien der Empfänger unterrichtet wird. Die Erhebung und Verarbeitung personenbezogener Daten der Biobank muss gegenüber dem Betroffenen transparent sein. Personenbezogene Daten sind grundsätzlich beim Betroffenen zu erheben. Außerdem sind die Betroffenenrechte, insbesondere das Auskunftsrecht des Betroffenen über seine Daten, ihre Herkunft und Empfänger sowie seine Berichtigungs- und Löschungsansprüche zu gewährleisten.

3.1.3.6 Datensicherheit

Die Verarbeitung personenbezogener Daten setzt die Implementierung von technischen und organisatorischen Regeln der Datensicherheit nach dem Stand der Technik voraus. Der Datenschutz ist nur gewährleistet, wenn die personenbezogenen Daten sicher verarbeitet werden. Die verantwortliche Stelle hat daher die Vertraulichkeit, die Verfügbarkeit und die Integrität der personenbezogenen Daten zu gewährleisten, indem sie die erforderlichen organisatorischen und technischen Maßnahmen trifft. Wegen der hohen Sensibilität ist eine hohe Schutzstufe erforderlich.

3.1.3.7 Wirksame Kontrolle

Die Datenverarbeitung muss einer internen und externen Kontrolle unterliegen. Die Verarbeitung personenbezogener Daten bedarf der Kontrolle durch interne Mechanismen und Institutionen wie den betrieblichen/behördlichen Datenschutzbeauftragten. Daneben sind externe Kontrollen in Form einer externen unabhängigen Kontrollinstitution wie den Aufsichtsbehörden (u. a. Landesbeauftragten / Bundesbeauftragten für den Datenschutz) bzw. der Ethikkommission nötig. Ein weiterer Mechanismus, die Einhaltung von Datenschutzanforderungen in der Praxis zu überprüfen, ist die Durchführung eines Datenschutzaudits.

3.2 Spenderschutz durch Datentreuhänderschaft

3.2.1 Überstaatliches Recht zur Datentreuhänderschaft

Völkerrechtliche oder supranationale Rechtsvorschriften, die sich im Detail zur Datentreuhänderschaft bei Biobankdaten äußern, sind nicht festgestellt worden. Es sind einzelne Regeln, Leitlinien und Empfehlungen vorhanden, die diese ansprechen bzw. den Schutz von Spenderrechten durch Dritte empfehlen. Dabei liegt der Fokus zu einem Teil auf dem Datenschutz, zum anderen Teil auf der Qualitätssicherung, die jedoch auch relevante Elemente für den Datenschutz beinhaltet. Mit dem Datenschutz-Ansatz verbindet sich der Leitbegriff des Spender schützenden Wächteramts („custodianship"), mit dem Qualitätssicherungs-Ansatz verbindet sich der Leitbegriff der Verfolgbarkeit („traceability") von Proben und Daten. Demgegenüber existieren eine Vielzahl an Regelungen und Empfehlungen zu den allgemeinen Anforderungen an die Biobank-Forschung. Zu den insoweit relevanten Erklärungen, Vereinbarungen und Berichte gehören die Erklärungen des Weltärztebundes, des Rats der Internationalen Organisationen für medizinische Wissenschaften, der UNESCO, des Europarats, der Europäische Union (EU) und der OECD.

3.2.1.1 Weltärztebund

Die Erklärung des Weltärztebundes (WMA) zu ethischen Grundsätzen für die medizinische Forschung am Menschen von 1964 in der Fassung von 2004[42] befasst sich mit Forschungen an einem erkrankten Patienten durch den behandelnden Arzt. Die ethischen Regeln über die Forschung am Menschen sollen aber ebenso auf die Forschung mit identifizierbarem menschlichem Material und identifizierbaren Daten angewandt werden[43]. Eine wesentliche Aussage ist, dass das Interesse des Patienten bei den Forschungen im Vordergrund zu stehen hat[44]. Diese Forderung wird in der Deklaration des Weltärztebundes zu ethischen Überlegungen in Bezug auf Gesundheitsdatenbanken[45] präzisiert:

- Es müssen Sicherheitsmaßnahmen vorhanden sein, die den unangemessenen oder unbefugten Zugang und die entsprechende Nutzung der Gesundheitsdaten der Betroffenen verhindern[46].
- Mit Hilfe von Auditsystemen müssen Zugriffsprotokolle geführt werden; diese Zugriffsprotokolle sollen den Patienten für eine eigene Nachprüfung zur Verfügung stehen[47].
- Daten für Sekundärzwecke[48] sollten anonymisiert oder pseudonymisiert genutzt werden[49].
- Als Verantwortlicher für Datenschutz und Datensicherheit[50] sollte jemand mit medizinischer Qualifikation eingesetzt werden[51]. Die Ärzte sind für den vertraulichen Umgang mit den Gesundheitsdaten persönlich verantwortlich und zur Rechenschaft verpflichtet. Die Sicherheit

---

[42] Deklaration des Weltärztebundes von Helsinki, Ethische Grundsätze für die medizinische Forschung am Menschen, verfügbar unter http://www.wma.net/e/policy/b3.htm.
[43] Deklaration des Weltärztebundes von Helsinki, Ethische Grundsätze für die medizinische Forschung am Menschen, A.1., Satz 2.
[44] Deklaration des Weltärztebundes von Helsinki, Ethische Grundsätze für die medizinische Forschung am Menschen, A.5.
[45] Deklaration des Weltärztebundes über ethische Erwägungen zu Gesundheitsdatenbanken, verfügbar unter http://www.wma.net/e/policy/d1.htm.
[46] Deklaration des Weltärztebundes über ethische Erwägungen zu Gesundheitsdatenbanken, Nr. 14.
[47] Deklaration des Weltärztebundes über ethische Erwägungen zu Gesundheitsdatenbanken, Nr. 15.
[48] Deklaration des Weltärztebundes über ethische Erwägungen zu Gesundheitsdatenbanken, Nr. 24.
[49] Deklaration des Weltärztebundes über ethische Erwägungen zu Gesundheitsdatenbanken, Nr. 24.
[50] Die Erklärung spricht vom „guardian of the health database".
[51] Deklaration des Weltärztebundes über ethische Erwägungen zu Gesundheitsdatenbanken Nr. 13.

beim Ablauf des Versands, Empfangs und der Speicherung der Daten muss die Ärzte überzeugen[52].

3.2.1.2 Rat der Internationalen Organisationen für medizinische Wissenschaften

Die Genfer Erklärung über ethische Leitlinien für die biomedizinische Humanforschung von 2002[53], die der Rat der Internationalen Organisationen für medizinische Wissenschaften (CIOMS[54]) gemeinsam mit der Weltgesundheitsorganisation verabschiedet hat, verlangt in ihrer Leitlinie 18 zur Sicherung der Privatsphäre des Betroffenen die Einrichtung sicherer Vorkehrungen für den Schutz der Vertraulichkeit der personenbezogenen Forschungsdaten. Dabei sollen dem Betroffenen die tatsächlichen und rechtlichen Grenzen des Schutzes sowie die Konsequenzen erklärt werden, die ein Bruch der Vertraulichkeit für ihn haben kann.

3.2.1.3 UNESCO

Die UNESCO will in ihrer Universellen Deklaration zum Schutz des menschlichen Genoms und der Menschenrechte vom 11.11.1997[55] das Spannungsverhältnis zwischen dem Humangenom als Zurechnungspunkt individueller Würde und als Gemeinschaftsgut des gemeinsamen Erbes der Menschheit rechtlich bestimmen. Sie erklärt, dass das menschliche Genom in seinem natürlichen Zustand kein Gegenstand des Gewinnstrebens sein soll[56]. Die Diskriminierung einer Person aus genetischen Gründen wird geächtet[57]. Nicht-anonyme genetische Daten, die zu Zwecken der Forschung verwandt werden, müssen auf gesetzmäßige Weise vertraulich behandelt werden[58]. Demgegenüber zielt die Internationale Erklärung über menschliche Gendaten vom 16.10.2003[59] der UNESCO auf den Schutz menschlicher Gen- und Genexpressionsdaten sowie diesbezüglicher Bioproben. Nach Art. 14 b der Erklärung sollen menschliche genetische Daten, menschliche Proteomikdaten und Bioproben, die mit einer identifizierbaren Person verbunden sind, gegenüber Dritten geheim gehalten werden. Ausnahmen hiervon sollen nur auf Grund eines Gesetzes zulässig sein, das mit den Menschenrechten vereinbar ist. Nach Art. 14 c sollen die o. g. Daten und Proben, die für Zwecke der wissenschaftlichen Forschung gesammelt werden, nur ausnahmsweise mit einer identifizierbaren Person verbunden sein. Wenn dieser Bezug gelöst wurde, sollten Vorsichtsmaßnahmen getroffen werden, um die Sicherheit von Proben und Daten sicherzustellen.

3.2.1.4 Europarat

Das „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108) – Europäische Datenschutzkonvention[60]“ ist in Deutschland am 1.10.1985 in Kraft getreten[61]. Danach sind für den Schutz personenbezogener Daten, die in automatisierten Dateien oder Datensammlungen gespeichert sind, geeignete

---

[52] Deklaration des Weltärztebundes über ethische Erwägungen zu Gesundheitsdatenbanken, Nr. 12.
[53] Abrufbar unter http://www.cioms.ch/frame_guidelines_nov_2002.htm.
[54] Council for International Organizations of Medical Sciences, Genf; abrufbar unter http://www.cioms.ch.
[55] Abrufbar als Datei http://unesdoc.unesco.org/images/0011/001102/110220e.pdf#page=47.
[56] Art. Nr. 4 der Universellen Deklaration zum Schutz des menschlichen Genoms und der Menschenrechte.
[57] Art. Nr. 6 Universellen Deklaration zum Schutz des menschlichen Genoms und der Menschenrechte.
[58] Art. Nr. 7 Universellen Deklaration zum Schutz des menschlichen Genoms und der Menschenrechte.
[59] Abrufbar unter http://unesdoc.unesco.org/images/0013/001331/133171e.pdf#page=45.
[60] Abrufbar unter http://conventions.coe.int/Treaty/ger/Treaties/Html/108.htm.
[61] Mittlerweile sind 38 Staaten der Europäischen Datenschutzkonvention beigetreten.

Sicherungsmaßnahmen gegen die zufällige oder unbefugte Zerstörung, gegen zufälligen Verlust sowie unbefugten Zugang, unbefugte Veränderung oder unbefugtes Bekanntgeben zu treffen[62]. Dem „Übereinkommen zum Schutz der Menschenrechte und der Menschenwürde im Hinblick auf die Anwendung von Biologie und Medizin: Übereinkommen über Menschenrechte und Biomedizin (SEV-Nr. 164) – Biomedizinkonvention“ des Europarats[63] ist Deutschland nicht beigetreten. Zusätzlich hat das Ministerkomitee des Europarats eine Empfehlung zur Forschung mit Biomaterial menschlichen Ursprungs und zu bevölkerungsbezogenen Biobanken (Empfehlung Rec(2006)4) erlassen[64]. Sie gilt nur für bevölkerungsbezogene (nicht krankheitsbezogene) Biobanken und umfasst alle Aktivitäten im Zusammenhang mit Biomaterial menschlichen Ursprungs, das für Forschungszwecke gelagert wird. Sie betrifft auch Biomaterial, das nicht für Forschungszwecke oder für einen anderen Forschungszweck entnommen wurde[65]. Die Empfehlung setzt Mindeststandards, die nicht unterschritten, zugunsten des Betroffenen aber überschritten werden dürfen[66].

Für Biobanken bzw. Biobankenprozesse sind folgenden Empfehlungen relevant:

- Die Mitgliedstaaten sollten die Einführung von Regelwerken guter Biobankpraxis fördern[67].
- Die für die Sammlung verantwortliche Person und/oder Einrichtung sollen benannt werden[68].
- Der Sammlungszweck und die Regeln über Vorhaltung, Nutzung und Weitergabe des Materials sollten spezifiziert und transparent festgelegt sein; es sollten klare Zugangs- und Nutzungsregeln festgelegt sein[69].
- Jede Probe sollte mit ihrer zugehörigen Einwilligung dokumentiert sein[70].
- Es soll ein Qualitätsmanagement eingerichtet werden, das die Bedingungen für die Gewährleistung von Sicherheit und Vertraulichkeit bei der Aufbewahrung und dem Umgang mit biologischem Material beinhaltet[71].
- Das Vorhaben der Errichtung oder der Umwidmung einer Sammlung zu einer populationsbezogenen Biobank sollte einer unabhängigen Prüfung unterzogen werden, die sicherstellt, dass die Regeln dieser Empfehlung beachtet werden[72].
- Jede Biobank sollte unabhängiger Aufsicht unterliegen, insbesondere um Rechte und Interessen der Personen sicherzustellen, die von der Aktivität der Biobank betroffen sind[73].
- Es sollten regelmäßige nicht anlassbezogene Audits (Prüfungen) durchgeführt werden, die den Zugang zu Proben und die Benutzung von Proben betreffen[74].

---

[62] Art. 7 der Europäischen Datenschutzkonvention.
[63] Abrufbar unter: http://conventions.coe.int/Treaty/ger/Treaties/Html/164.htm.
[64] Recommendation Rec(2006)4 on research on biological materials of human origin vom 15. März 2006, abrufbar unter: https://wcd.coe.int/ViewDoc.jsp?id=977859 (englisch) bzw. unter http://www.bmj.bund.de/files/-/1440/Empfehlung%20-%20deutsch.pdf als nicht-amtliche Fassung in deutscher Sprache.
[65] Art. 2 und 3 der Empfehlung Rec(2006)4.
[66] Art. 9 der Empfehlung Rec(2006)4.
[67] Art. 4 der Empfehlung Rec(2006)4.
[68] Art. 14 Nr. 2 der Empfehlung Rec(2006)4.
[69] Art. 14 Nr. 2 und 4 der Empfehlung Rec(2006)4.
[70] Art. 14 Nr. 3 der Empfehlung Rec(2006)4.
[71] Art. 14 Nr. 5 der Empfehlung Rec(2006)4.
[72] Art. 18 der Empfehlung Rec(2006)4.
[73] Art. 19 Nr. 1 der Empfehlung Rec(2006)4.
[74] Art. 19 Nr. 2 der Empfehlung Rec(2006)4.

- Es sollten Prozeduren für die Übertragung und die Schließung einer Biobank entwickelt werden[75].
- Bevölkerungsbezogene Biobanken sollten über ihre zurückliegenden und ihre geplanten Vorhaben mindestens jährlich berichten, wenn nicht ein häufigerer Bericht angemessen ist[76].
- Die Forschung unter Zuhilfenahme von Biobanken sollte unabhängiger Kritik unterliegen[77].

3.2.1.5 Europäische Union

Die Datenschutzrichtlinie 95/46 der Europäischen Union (EU, DSRL) gibt einen Mindeststandard vor, ohne das ggf. existierende höhere Niveau zu beschränken. Es werden mehrere Verarbeitungsgrundsätze aufgestellt, die bei jeder Datenerhebung und –verarbeitung beachtet werden müssen, darunter auch die Zweckbindung (Art. 6 (1) (b) DSRL), die Rechtmäßigkeit der Datenverarbeitung (Art. 7(a), 8 (2) (a), 10 und 11 DSRL), das Gebot der Datenvermeidung / Datensparsamkeit (Art. 6 und 7 DSRL), die Zuweisung von Verantwortlichkeiten für den jeweiligen Datenverarbeitungsschritt (Art. 2(d) und Art. 17 (2)-(4) DSRL), die Verhältnismäßigkeit (Art. 6 (1) (c) DSRL) sowie der Erforderlichkeit (Art. 7 DSRL).

Gesundheitsdaten – darunter fallen auch genetische Daten, soweit sie nicht andere als gesundheitliche Zustände beinhalten[78] – verlangen gem. Art. 8 DSRL ein erhöhtes Schutzniveau. Deren Verarbeitung ist grundsätzlich verboten und nur bei Vorliegen bestimmter Umstände gestattet. Zugleich enthält die Richtlinie mehrere Privilegierungen für die Datenverarbeitung zu wissenschaftlichen Zwecken, die jedoch nur geltend gemacht werden können, wenn von den Mitgliedstaaten geeignete Garantien vorgesehen sind. Grundsätzlich ist eine Verarbeitung der Daten zu Forschungszwecken auf der Grundlage einer Einwilligung zulässig, soweit die Anforderungen an die Einwilligung eingehalten, sie insbesondere hinreichend bestimmt ist und geeignete Garantien des Mitgliedstaates vorgesehen werden. Dabei gilt gem. Art. 6 Abs. 1 lit. b Satz 2 DSLR die Vermutung, dass die Weiterverarbeitung zu wissenschaftlichen Zwecken grundsätzlich nicht als unvereinbar mit dem Ursprungszweck zu sehen ist. Eine Forschungserleichterung im Sinne eines Verzichts auf die Einwilligung in die Datenverarbeitung ergibt sich aus Art 8 Abs. 4 DSRL. Danach ist eine Nutzung von personenbezogenen sensiblen Daten zulässig, wenn ein wichtiges öffentliches Interesse vorliegt. Nach den Erwägungsgründen ist die wissenschaftliche Forschung ein solches öffentliches Interesse.[79] Daneben statuiert die Richtlinie Benachrichtigungspflichten, soweit die Daten nicht bei dem Betroffenen erhoben werden sowie Auskunftspflichten und Betroffenenrechte, Art. 11, 12 und 13 DSRL.

3.2.1.6 OECD

3.2.1.6.1 Creation and Governance of Genetic Resource Databases (2006)

[75] Art. 19 Nr. 3 der Empfehlung Rec(2006)4.
[76] Art. 19 Nr. 4 der Empfehlung Rec(2006)4.
[77] Art. 24 Nr. 1 der Empfehlung Rec(2006)4.
[78] Antonow, Der rechtliche Rahmen der Zulässigkeit für Biobanken zu Forschungszwecken, S. 82ff.
[79] Erwägungsgrund 34.

Ende 2006 wurde das OECD-Papier zur **Errichtung und Führung von Humangenomdatenbanken**[80] („Creation and Governance of Human Genetic Research Databases“) für den Bereich der genetischen Forschung verfasst. Formal handelt es sich um ein Diskussionspapier. Es weist auf die hohe Datenschutzrelevanz von Biobanken hin[81] und führt aus, dass ein Spender auch nach Entfernung der ihn identifizierenden Daten leicht identifizierbar sein kann, und zwar direkt oder durch Zugriff auf andere öffentlich zugängliche oder sonst beschaffbare Daten über den Betroffenen. Deshalb müssen Methoden zum Schutz von Privatsphäre und Vertraulichkeit des Betroffenen eine bedeutende Rolle beim Betrieb von Biobanken spielen:

- Anonymisierung oder Pseudonymisierung der Daten des Betroffenen sind unerlässlich.
- Zur betrieblichen Sicherstellung der Wirksamkeit dieser Maßnahmen muss ein „Custodian of Code Registry“[82] eingerichtet sein. Diese Person sollte unter besonderer Schweigepflicht stehen und die Verletzung dieser Pflicht sollte strafbewehrt sein.
- Es sollte geprüft werden, ob Computer, die zur Sicherung der Vertraulichkeit der Daten des Betroffenen eingesetzt werden, besser unvernetzt bleiben. Dies bedeutet, dass IT, die zur Sicherung der Vertraulichkeit von Spenderinnen und Spendern eingesetzt wird, sich nach Technik und Organisation in einer klar und verantwortlich abgegrenzten Zone besonderer Sicherheit befinden muss.
- Es werden Regelungen zum Probeneigentum[83] und zur Einhaltung der Vorgaben der informierten Einwilligung verlangt.[84]
- Das Recht des Spenders, von der Teilnahme an der Biobank zurückzutreten, muss gewährleistet sein.
- Es muss kommunizierte Regeln darüber geben, wann welche Informationen aus der Forschung zurück in die Biobank gehen und wann solche Informationen an den Spender weiterzuleiten sind[85].
- Die Fortbildung der Forscher muss ebenso gewährleistet sein wie die des Biobankpersonals[86].
- Es muss Ethik- und Kontrollkomittees geben[87].
- Die Sicherheit der Biobank muss besonders geregelt sein: Der Zugang zu personenbezogenen Daten muss besonders gesichert sein.
- Das Herausgeben von Daten und der Datenzugang müssen sich an dem Prinzip der Datensparsamkeit orientieren.
- Personenbezogene Daten müssen verschlüsselt werden.
- Es muss ein auditierbares Log der Benutzer, Abfragen und Ausgaben geben[88].

---

[80] OECD, Creation and Governance of Human Genetic Research Databases, OECD, Paris 2006, abrufbar unter http://www.oecdbookshop.org/oecd/display.asp?lang=EN&sf1=identifiers&st1=932006091e1.
[81] OECD, Creation and Governance of Genetic Resource Databases (2006), S. 65 ff.
[82] OECD, Creation and Governance of Genetic Resource Databases (2006), S. 111
[83] OECD, Creation and Governance of Genetic Resource Databases (2006), S. 88.
[84] OECD, Creation and Governance of Genetic Resource Databases (2006), S. 89 ff.
[85] OECD, Creation and Governance of Genetic Resource Databases (2006), S. 96 f.
[86] OECD, Creation and Governance of Genetic Resource Databases (2006), S. 99ff.
[87] OECD, Creation and Governance of Genetic Resource Databases (2006), S. 105 ff.
[88] OECD, Creation and Governance of Genetic Resource Databases (2006), S. 111 ff., 113.

- Bei der Aufgabe einer Biobank müssen besondere Regeln für die zuverlässige und integre Erhaltung oder notfalls für die Vernichtung der Sammlung sorgen[89].

Vorschläge für Vorgaben zu Audits oder zur staatlichen Auditregulierung (etwa durch freiwillige Gütesiegel) sind nicht enthalten.

3.2.1.6.2 Best-Practice-Guidelines for Biological Resource Centres

2007 erschienen die OECD Best Practice Guidelines for Biological Resource Centres (BRC)[90]. Sie befürworten für den Bereich der Humanforschung das Qualitätsprinzip der Verfolgbarkeit vom Spender bis zum Forscher[91] sowie das Prinzip der Vertraulichkeit[92]. Das Papier spricht sich zudem für ein differenziertes System aus internen Audits, Audits durch Kunden oder Lieferanten und Audits durch eine zertifizierte unabhängige dritte Stelle aus[93]. Zur allgemeinen Etablierung von Audits wird der nationalstaatlichen Regulierung die Orientierung an den Normen ISO 9001, ISO 17021 und ISO 19011 empfohlen[94].

3.2.1.6.3 Draft-Guidelines for Human Biobanks and Genetic Research Databases

Im Mai 2008 erschien der Diskussionsentwurf von Guidelines for Human Biobanks and Genetic Research Databases[95]. Der Entwurf enthält in seinem ersten Teil Principles und Best Practices, die in einem zweiten Teil erläutert sind. Der Entwurf wurde über das Internet zur Diskussion gestellt. Auf der Grundlage der bis zum 16. Mai 2008 eingegangenen Diskussionsbeiträge wird die OECD voraussichtlich in 2009 endgültige Guidelines erlassen. Der Entwurf bezieht sich ausdrücklich nur auf die Forschung, nicht etwa auf den klinischen Bereich oder sonstige andere Bereiche[96].
Der Diskussionsentwurf enthält die folgenden Leitlinien für Biobanken:

- Die Führung der Biobank sollte dafür Sorge tragen, dass ihr Betrieb die Forschung in ihrem gesetzlichen und ethischen Kontext fördert[97]. Die Biobank sollte dafür Protokolle und Prozesse vorhalten, die die Privatsphäre der Spender schützt[98].
- Der gegenwärtige und künftige Zweck der Biobank sollte klar formuliert und so früh und breit kommuniziert werden, wie dies möglich ist, besonders aber nicht ausschließlich an mögliche Spender und Nutzer (Forscher)[99]. Die Finanzierung der Biobank sollte explizit und transparent gemacht werden[100]. Die Biobank sollte einen breiten Diskussionsprozess mit allen relevanten Gruppen pflegen[101]. Wo die Möglichkeit besteht, dass eine Biobank privates oder

[89] OECD, Creation and Governance of Genetic Resource Databases (2006), S. 117 f.
[90] Abrufbar unter: http://www.oecd.org/dataoecd/7/13/38777417.pdf.
[91] OECD, BRC, S. 74.
[92] OECD, BRC, S. 37, 76, 78.
[93] OECD, BRC, S. 23, 96 ff.
[94] OECD, BRC, S. 98.
[95] Abrufbar unter: http://www.oecd.org/document/50/0,3343,en_2649_34537_37646258_1_1_1_1,00.html.
[96] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, Scope, S. 6.
[97] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 1.A, S. 6.
[98] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 1.5., S. 6.
[99] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 2.A, S. 7.
[100] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 2.D, S. 7.
[101] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 2.2, S. 7.

ausländisches Kapital einwirbt oder mit der Verfolgung kommerzieller Interessen beginnt, sollte dies den Spendern vermittelt werden[102].

- Unabhängige Audit-Mechanismen müssen vorhanden sein, die insbesondere die einwilligungsgemäße Verwendung von Proben und Daten prüfen.[103]
- In den Draft-Guidelines fehlt das explizite Erfordernis eines schriftlichen Datenschutzkonzepts.
- Die Spendereinwerbung sollte auf Augenhöhe mit dem Spender und ohne Zwangswirkung erfolgen[104]. Die Rückkopplung ungesicherter Forschungserträge an Spender soll unterbleiben. Dies muss dem Spender in der Spenderinformation erläutert werden.[105] Die Biobank soll die Verfolgbarkeit von Proben und Daten sicherstellen, damit es möglich ist, dass der Spender sein Recht ausüben kann, seine Einwilligung zurückzunehmen.[106]
- Audit-Mechanismen müssen gleichermaßen Qualität und Spendervertraulichkeit zum Ziel haben[107]. Prozesse der Probenverfolgung und des Qualitäts-Audits müssen in ihrer Ausgestaltung zum Grundsatz der Spendervertraulichkeit passen.[108] Biobanken müssen sich in einer klaren Policy dazu erklären, ob sie die Daten der Biobank aus den Erträgen der Forschung anreichern.[109]. Die Biobank soll für ihre betrieblichen Prozesse Standard Operating Procedures (SOP) entwickeln[110].
- Für den Datenschutz und den Schutz der Vertraulichkeit sollte in der Biobank eine verantwortliche Position identifiziert sein[111]. Darüber, wie Datenschutz und Vertraulichkeit geschützt werden, sollen Information angeboten werden[112]. Datenschutz und Vertraulichkeit sollte die Biobank durch kombinierte Maßnahmen datenschutzfördernder Technik sicherstellen. Dazu gehören Zonen besonderer Datensicherheit und IT-Systeme, die Zuordnungsregeln medizinischer Daten und Proben besonders geschützt verwalten (elektronischer Datentreuhänder, als „honest broker systems“ bezeichnet).[113] Dabei sollte der Datenschutz besondere Maßnahmen der Trennung identifizierender Daten von Daten zur Beforschung enthalten.[114] Maßnahmen des Datenschutzes und der Vertraulichkeit müssen sich gleichermaßen auf Daten wie auf Proben beziehen.[115]
- Auch bei der Bereitstellung von Daten und Proben zur Beforschung sollte die Privatsphäre der Spender und die Vertraulichkeit ihrer Daten besonders beachtet werden.[116] Proben sollten zur Beforschung nur herausgegeben werden, wenn die Privatsphäre des Spenders angemessen geschützt ist und die Vertraulichkeit der Daten, die Sicherheit und zuverlässige

[102] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 2.7, S. 8.
[103] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 3.J, S. 9.
[104] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 4.A, S. 15.
[105] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 4.J, S. 17.
[106] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 4.11, S. 19.
[107] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 5.D, S. 13.
[108] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 5.D, S. 20.
[109] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 5.E, S. 20 sowie 9.D, S. 31.
[110] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 5.G, S. 20.
[111] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 6.1, S. 15.
[112] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 6.3, S. 15.
[113] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 6.4, S. 16.
[114] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 6.5, S. 16.
[115] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 6.8, S. 16.
[116] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 7.B, S. 17.

labortechnische Abwicklung gewährleistet sind.[117] Zugriffe von dritter Seite auf die Biobank können auf gesetzlicher Grundlage ausgeschlossen werden.[118]

- Die Biobank muss sich unmissverständlich dazu erklären, ob und welche Rechte Spender an Proben und Daten zurückbehalten.[119] Diese Erklärung sollte Bestandteil der Spendereinwilligung sein. Die Biobank soll eine Erklärung dazu haben, ob sie ihre Daten mit Erträgen aus der Forschung anreichert[120]. Weiter muss sie bekannt machen, ob und wie sie Forschungserträge kommerzialisieren will. Hier fällt auf, dass die Begrifflichkeit des „Custodian" gegenüber dem Workshop-Papier aus 2006 „Creation and Governance of Genetic Resource Databases"[121], ihren Gegenstand gewechselt hat. Ging es dort um die Bewachung der Trennung identifizierender Daten von Studiendaten, so geht es hier um den Gesichtspunkt, ob und welche Rechte der Spender an Forschungserträgen erhält und ob in der Biobank Zusatzwissen aufgebaut wird, das den Spender in der Zukunft möglicherweise re-identifizieren kann. Eine sachliche Änderung ist mit diesem Wandel in der Begriffsverwendung nicht verbunden. Die ursprüngliche Funktion des Datentreuhänders als einer betrieblichen Rolle institutionell verstärkter Datentrennung hat nun die „responsible position for ensuring the protection of data and privacy".[122]
- Sobald die Sammlung einer Biobank nicht mehr erforderlich ist oder sobald ihr wissenschaftlicher Wert entfallen ist, sollten Proben und Daten in angemessener Weise und unter Beachtung des Datenschutzes vernichtet werden.[123] Dies soll so geschehen, dass jegliche Rückgewinnung personenbeziehbarer Informationen ausgeschlossen ist.[124]

Im Hinblick auf den 2007 vorgelegten Bericht aus dem Jahr 2003 „Genetic Testing – A Survey of Quality Assurance and Proficiency Standards" zu den Verhältnissen verbesserungsbedürftiger Qualitätskultur in der Forschung verweist der Entwurf der Guidelines for Human Biobanks and Genetic Research Databases aus 2008 lediglich auf die Best-Practice-Guidelines for Biological Resource Centres (BRC) aus 2007 (s.o.). Dies bedeutet, dass weiterhin ein Bedarf an internen und externen Audits festgestellt wird, ohne dass detaillierte Empfehlungen abgeben werden.

3.2.2 Regeln zur Datentreuhänderschaft und Anforderungen an vertrauenswürdige Biobanken in ausgewählten europäischen Ländern

3.2.2.1 Schweiz

3.2.2.1.1 Allgemeine Datenschutzgesetze: Bundesgesetz über den Datenschutz

Ähnlich wie in Deutschland regelt das Datenschutzgesetz des Bundes (DSG) den Datenschutz für die Bundesbehörden und für den privaten Bereich; auf die kantonalen Behörden ist das jeweilige

[117] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 7.J, S. 17.
[118] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 7.K, S. 17.
[119] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 9.A, S. 30.
[120] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 9.D, S. 31.
[121] OECD, Creation and Governance of Genetic Resource Databases (2006), S. 111.
[122] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 6.1., S.15.
[123] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 10.D, S. 22.
[124] OECD, Draft-Guidelines for Human Biobanks and Genetic Research Databases, 10.F, 10.G., S. 22.

kantonale Datenschutzgesetz anwendbar. Neben den allgemeinen Grundsätzen ist im DSG eine ausdrückliche Informationspflicht der Betroffenen vorgesehen: Werden schützenswerte Personendaten verarbeitet, dann müssen die betroffenen Personen aktiv durch den Inhaber der Datensammlung informiert werden[125]. Zu den schützenswerten Personendaten zählen in der Schweiz zusätzlich zu ähnlichen Definitionen in Deutschland und Österreich auch jegliche Daten, die eine Profilbildung erlauben.[126] Der Datenschutzbeauftragte führt ein Register der Datensammlungen, das über Internet zugänglich ist und von jeder Person einsehbar ist[127].

3.2.2.2.2 Bundesgesetz über genetische Untersuchungen beim Menschen

Das Schweizer Bundesgesetz über genetische Untersuchungen beim Menschen (GUMG) aus dem Jahr 2004 bestimmt, unter welchen Voraussetzungen im medizinischen Bereich, im Arbeitsbereich, im Versicherungsbereich und im Haftpflichtbereich genetische Untersuchungen beim Menschen durchgeführt werden dürfen.[128] Es enthält keine Vorgaben zur Datenverarbeitung zum Zwecke der Forschung. Es beinhaltet im zweiten Abschnitt die allgemeinen Grundsätze für genetische Untersuchungen, die die Diskriminierung des Einzelnen wegen seines Erbguts verbieten[129], die Zustimmung der betroffenen Person nach hinreichender Aufklärung für eine genetische Untersuchung zur Voraussetzung macht[130], das Recht des Einzelnen auf Nichtwissen festlegt, sowie die Bearbeitung genetischer Daten dem Berufsgeheimnis und den allgemein gültigen Datenschutzbestimmungen unterstellt[131].

3.2.2.2.3 Richtlinien und Empfehlungen der Schweizer Akademie der Medizinischen Wissenschaften

Regeln zur Datentreuhänderschaft sind in den Medizinisch-ethischen Richtlinien und Empfehlungen der Schweizer Akademie der Medizinischen Wissenschaften (SAMW) vom 23. Mai 2006 zur „Gewinnung, Aufbewahrung und Nutzung von menschlichem biologischem Material für Ausbildung und Forschung“ (SAMW Richtlinien und Empfehlungen zu Biobanken) [132] enthalten. Diese Regelwerke des SAMW sind Beispiele für sog. Soft Laws, d. h. Normen ohne zwingende Verbindlichkeit. In der Schweiz werden jedoch die SAMW-Richtlinien bis zum Inkrafttreten des Humanforschungsgesetzes Wirkung entfalten. Die Richtlinien wenden sich an alle Betreiber und Nutzer von Biobanken und anderen Sammlungen menschlichen biologischen Materials und legen Anforderungen an Biobanken fest:

Jede Biobank muss insbesondere dafür sorgen, dass

- sie über qualifiziertes Personal, geeignete Strukturen und Material verfügt,

[125] Art. 7a DSG.
[126] Art. 3c DSG.
[127] Art. 11a DSG; das Register ist abrufbar unter https://www.datareg.admin.ch/WebDatareg/search/SearchSimple.aspx.
[128] Art. 1 GUMG.
[129] Art. 4 GUMG.
[130] Art. 5 GUMG.
[131] Art. 7 GUMG.
[132] Abrufbar unter http://www.samw.ch/docs/Richtlinien/d_RL_Biobanken.pdf.

- für die Aufbewahrung und Nutzung der Proben ein angemessenes Qualitätssicherungssystem besteht,
- die Rechte der Spender, insbesondere der Datenschutz, gewährleistet sind,
- die Weiterleitung von Proben unter Wahrung der Persönlichkeitsrechte der Spender erfolgt,
- ein Reglement besteht, welches die wesentlichen Punkte regelt[133].

Zur Weitergabe von Proben und Daten ist festgelegt:

- Proben von menschlichem biologischem Material dürfen nur in reversibel oder irreversibel anonymisierter Form weitergeleitet werden. Bei reversibel anonymisierten Proben darf der Empfänger keinen Zugriff auf den Schlüssel haben.
- Jede Weitergabe (von Proben oder von Proben und Daten) muss nachvollziehbar dokumentiert und in einem Transfervertrag (Material Transfer Agreement, MTA) geregelt werden.
- Die Wahrung der Persönlichkeitsrechte des Spenders (insbesondere auch das Recht auf Widerruf) muss bei jeder Weitergabe von Proben und Daten gewährleistet sein.
- Eine Weitergabe ist nur zulässig, wenn sichergestellt ist, dass die Standards gemäß den vorliegenden Richtlinien eingehalten werden.
- Wird eine Biobank als Ganzes übertragen, muss der nachfolgende Träger die Anforderungen gemäß den Richtlinien erfüllen[134].

Zur Dokumentation bestimmt sie:

- Das Reglement soll die Organisation, die Verantwortlichkeiten und den Anwendungsbereich der Biobank regeln.
- Es soll insbesondere auch Bestimmungen betreffend die Herkunft der aufbewahrten Proben, den Verwendungszweck sowie den Kreis der Zugangsberechtigten und den Voraussetzungen für den Zugang enthalten.
- Das Reglement soll die Integrität der Biobank schützen.
- Es empfiehlt sich, für mehrere Biobanken innerhalb einer Institution (Spital, Forschungszentrum usw.) grundsätzlich dieselben Reglements vorzusehen und sie einer gemeinsamen Leitung zu unterstellen[135].

An die Forschung mit menschlichem biologischem Material sind weitere Forderungen gestellt, die u. a. Forschungsprojekte, die Aufklärung und Einwilligung der Spender, den Widerruf der Einwilligung, die nachträgliche Information über relevante Ergebnisse, die Weitergabe von Proben und Daten betreffen.

Unter „Datenschutz“ ist die Datentreuhänderschaft ausdrücklich erwähnt:

---

[133] SAMW Richtlinien und Empfehlungen zu Biobanken, Punkt 3.
[134] SAMW Richtlinien und Empfehlungen zu Biobanken, Punkt 3.3.
[135] SAMW Richtlinien und Empfehlungen zu Biobanken, Punkt 3.4.

- Die Daten und Proben sollen durch angemessene technische und organisatorische Maßnahmen vor missbräuchlicher Verwendung wirksam geschützt werden. Dies gilt sowohl für die Aufbewahrung in der Biobank als auch für die Nutzung der Daten und Proben.
- Zum Schutz des Spenders sollte die Kodierung der Proben so früh wie möglich, spätestens aber bei Aufnahme in die Biobank erfolgen.
- Bei reversibel anonymisierten Proben besteht nur noch eine indirekte Verbindung zum Spender. Der Probe wird ein Kode zugeordnet. Der Zugriff auf die personenbezogenen Daten ist nur mit dem Kodierungsschlüssel möglich. Dieser ist von den Daten getrennt aufzubewahren und zu verwalten. Doppelt verschlüsselte Proben enthalten einen zweiten Schlüssel. Der Schlüssel zu diesem zweiten Kode liegt bei einer unabhängigen Stelle. Der Kodierungsschlüssel sollte in der Hand eines deklarierten Geheimnisträgers sein. Dieser sollte nicht direkt an der Forschung mit den Proben und Daten der Biobank beteiligt sein.
- Bei irreversibel anonymisierten Proben werden die personenbezogenen Daten so verändert, dass die Informationen über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten Person zugeordnet werden können, respektive das Risiko einer Re-Individualisierung äußerst gering ist, weil der Aufwand unverhältnismäßig groß wäre.
- Sowohl im Interesse der Patienten als auch im Interesse der Forschung sollten Proben und Daten nach Möglichkeit nicht irreversibel anonymisiert werden. Für den Patienten bedeutet die irreversible Anonymisierung, dass ihm relevante Ergebnisse im Allgemeinen nicht mehr mitgeteilt werden können; für die Forschung, dass die Proben und Daten an Aussagekraft verlieren.

3.2.2.2.4 Entwurf eines Schweizer Humanforschungsgesetzes (HFG)

In dem Entwurf sind bestimmte Anforderungen an die Einwilligung als Grundlage jedes Forschungsvorhabens sowie spezielle Anforderungen an Biobanken vorgeschlagen worden.

Zur Einwilligung:

- Der betroffenen Person ist zwischen Aufklärung und Einwilligung eine angemessene Bedenkfrist zu gewähren[136].
- Die Betroffenen müssen über Zweck, Dauer und Verlauf, die voraussehbaren Risiken und Belastungen, den erwarteten Nutzen für den Spender oder andere Personen, die Maßnahmen zum Schutz der erhobenen Daten sowie über ihre Rechte aufgeklärt werden[137].
- Die Betroffenen haben das Recht, ohne Angabe von Gründen die Teilnahme an einem Forschungsprojekt zu verweigern.[138]
- Die Betroffenen haben das Recht, auf Informationen verzichten. Führt ein Forschungsprojekt zu Ergebnissen, die zur Feststellung, Behandlung oder Verhinderung von bestehenden oder

[136] Art. 8 Abs. 1 HFG-Entwurf.
[137] Art. 8 Abs. 2 HFG-Entwurf.
[138] Art. 9 HFG-Entwurf.

künftig drohenden, schweren Krankheiten führen können, hat die betroffene Person das Recht, auf eine entsprechende Information zu verzichten[139].

- Die betroffene Person kann formlos und ohne Angaben von Gründen ihre bereits gegebene Einwilligung jederzeit widerrufen.[140]

Zur Biobank:

- Die Biobank hat in schriftlicher Form Folgendes festzulegen.
  - Sie hat den Zweck der Biobank näher zu bestimmen. Mit dem Zweck wird der Forschungsbereich, für den die gespeicherten biologischen Materialien und Personendaten zur Verfügung gestellt werden, umschrieben. Es muss z. B. festgehalten werden, ob mit Hilfe der Biobank Krebserkrankungen oder Herz-Kreislauf-Krankheiten erforscht werden, oder ob epidemiologische Forschung betrieben wird.
  - Sie muss die Aufnahmekriterien, die Verwendung und die Aufbewahrungsdauer für die Biobank festlegen. Die Aufnahmekriterien stellen sicher, dass nur dem Zweck der Biobank entsprechende biologische Materialien und Daten aufgenommen werden. Darüber hinaus müssen Kriterien festgehalten werden, wie die biologischen Materialien und Personendaten genutzt und wie lange sie aufbewahrt werden sollen.
  - Die Organisation der Biobank ist festzulegen und insbesondere die Verantwortlichkeiten zu bezeichnen Es muss z. B. festgelegt werden, wie die Aufsicht und Kontrolle über die Biobank organisiert sowie die Einhaltung des Qualitätsmanagements sichergestellt werden sollen.
  - Sie muss die Bedingungen für die Weitergabe von Proben an Dritte festlegen, bevor die Biobank in Betrieb genommen wird. Biobanken als Mittel zur Realisierung von Forschungsprojekten werden von verschiedenen Forschenden bezüglich der Herausgabe von biologischen Materialien und Daten angefragt. Zur Verhinderung missbräuchlicher Verwendungen, zur Nachverfolgbarkeit und zur Kontrolle über die Weitergabe von biologischen Materialien und Personendaten ist festzuhalten, unter welchen Voraussetzungen die Weitergabe erfolgt und in welcher Form sie dokumentiert wird. Geregelt werden müssen auch die Kosten, die bei der Weitergabe von Materialien an Dritte anfallen.
  - Sie hat darzulegen, wie die Einhaltung des Datenschutzes gewährleistet wird. Damit die Privatsphäre der betroffenen Personen geschützt ist, müssen die biologischen Materialien und Personendaten durch geeignete Maßnahmen insbesondere vor missbräuchlichen Zugriffen geschützt werden[141].
- Der Betrieb von Biobanken ist bewilligungs- bzw. meldepflichtig.[142]
- Die bewilligten Forschungsprojekte sowie eine Zusammenfassung deren Ergebnisse sind in einem öffentlich zugänglichen Register aufzunehmen.[143]

---

[139] Art. 11 HFG-Entwurf.
[140] Art. 12 Abs. 1 HFG-Entwurf.
[141] Art. 48 HFG-Entwurf
[142] Art. 75 und 58 HFG-Entwurf.
[143] Art. 72 Abs. 1 HFG-Entwurf.

Regelungen zur Datentreuhänderschaft enthält der Entwurf nicht. Mit einer Verabschiedung des Humanforschungsgesetzes für die Schweiz ist nicht vor 2010 zu rechnen[144].

3.2.2.2 Österreich

3.2.2.2.1 Allgemeines Datenschutzgesetz

In Österreich gilt das Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000). Dieses enthält neben allgemeinen Vorschriften besondere Bestimmungen zur Publizität der Datenverarbeitung.[145] Bei der Datenschutzkommission ist ein Register der Datenanwendungen zum Zweck der Prüfung ihrer Rechtmäßigkeit und zum Zweck der Information der Betroffenen eingerichtet[146]. Jeder Auftraggeber (d. h. die verantwortliche, Daten verarbeitende Stelle) hat vor Aufnahme einer Datenanwendung eine Meldung an die Datenschutzkommission zu erstatten. Ausnahmen gelten u. a. bei Standardanwendungen. Inhalt der Meldungen sind u. a. die Zweck der Datenverarbeitung und ihre Rechtsgrundlagen[147].

Weiter enthält das Gesetz eine Forschungsklausel[148]. Diese bestimmt, dass bei Datenanwendungen für Zwecke wissenschaftlicher Forschung, die personenbezogene Daten zum Ziel haben, Daten, die nicht öffentlich zugänglich sind, nur gemäß besonderen gesetzlichen Vorschriften oder mit Zustimmung des Betroffenen oder mit Genehmigung der Datenschutzkommission verwendet werden dürfen. Sollen sensible Daten übermittelt werden, muss ein wichtiges öffentliches Interesse an der Untersuchung vorliegen; weiter muss gewährleistet sein, dass die Daten beim Empfänger nur von Personen verwendet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verlässlichkeit sonst glaubhaft ist. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten, notwendig ist.

Auch in jenen Fällen, in welchen gemäß den vorstehenden Bestimmungen die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in personenbezogener Form zulässig ist, ist der direkte Personenbezug unverzüglich zu verschlüsseln. Der Personenbezug der Daten ist gänzlich zu beseitigen, sobald er für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig ist.

3.2.2.2.2 Gentechnikgesetz

Außerdem ist in Österreich das Gentechnikgesetz (GTG) in Geltung, das in seinem 4. Abschnitt Regelungen zur Genanalyse und Gentherapie am Menschen getroffen hat.

---

[144] Mund, Biobanks and Legislation in Switzerland – a Data Protection Perspective, Journal of International Biotechnology Law (JIBL), Vol. 4 (2007), S. 198 ff., S. 207.
[145] §§ 16-25 DSG 2000.
[146] § 16 DSG 2000.
[147] §§ 17, 19 DSG 2000.
[148] § 46 DSG 2000.

- Danach dürfen genetische Analysen am Menschen für wissenschaftliche Zwecke und zur Ausbildung nur mit ausdrücklicher und schriftlicher Zustimmung des Probenspenders oder an anonymisierten Proben durchgeführt werden. Eine Probe, die wissenschaftlichen Zwecken dient, gilt auch dann als anonymisiert, wenn sie ohne Namen nur mit einem Code versehen ist und dieser ausschließlich in der jeweiligen Einrichtung mit dem Namen des Probenspenders in Verbindung gebracht werden kann[149].
- Ergebnisse aus genetischen Analysen dürfen nur dann vernetzt oder veröffentlicht werden, wenn durch geeignete Maßnahmen sichergestellt ist, dass der Probenspender nicht bestimmbar ist[150].
- Ein schriftlicher Widerruf der Zustimmung ist jederzeit möglich. In diesem Fall dürfen diese Daten für neue Verwendungszwecke ab dem Zeitpunkt des Widerrufs nicht mehr herangezogen werden.[151]
- Arbeitgebern und Versicherern einschließlich deren Beauftragten und Mitarbeitern ist es verboten, Ergebnisse von genetischen Analysen von ihren Arbeitnehmern, Arbeitsuchenden oder Versicherungsnehmern oder Versicherungswerbern zu erheben, zu verlangen, anzunehmen oder sonst zu verwerten. Von diesem Verbot sind auch das Verlangen nach Abgabe und die Annahme von Körpersubstanz für genanalytische Zwecke umfasst[152].
- Der untersuchten Person ist Einsicht in alle sie betreffenden Daten zu gewähren.
- Der untersuchten Person sind unerwartete Ergebnisse mitzuteilen, die von unmittelbarer klinischer Bedeutung sind oder nach denen sie ausdrücklich gefragt hat. Diese Mitteilung ist insbesondere dann, wenn die untersuchte Person nicht danach gefragt hat, so zu gestalten, dass sie auf die untersuchte Person nicht beunruhigend wirkt; in Grenzfällen kann diese Mitteilung gänzlich unterbleiben.
- Daten in nicht anonymisierter Form dürfen für einen anderen als den Zweck, für den sie ursprünglich erhoben worden sind, nur mit ausdrücklicher und schriftlicher Zustimmung der untersuchten Person verwendet werden.
- Daten dürfen nur den gesetzlich bestimmten Personen übermittelt werden[153].
- Der Bundesminister für Gesundheit und Frauen hat ein elektronisches Register einzurichten, in dem alle zugelassenen Einrichtungen zur Durchführung von genetischen Analysen (Genanalyseregister), somatischen Gentherapien am Menschen (Gentherapieregister) und angebotenen Ringversuche (Ringversuchsregister) zu verzeichnen sind.

Ausdrückliche Vorschriften zur Datentreuhänderschaft bestehen nicht.

3.2.2.3 Island

In Island gilt für die (allgemeine) Datenverarbeitung von personenbezogenen Daten The Data Protection Act of Iceland sowie als bereichsspezifisches Recht im Medizinbereich The Act on the Rights of Patients no. 74/1997. Speziell für Biobanken kommt der im Jahr 2000 erlassene Act on Biobanks no 110/2000 (AoB) zur Anwendung, der die Sammlung (Erhebung), Speicherung,

[149] Art. 66 Abs. 1 GTG.
[150] Art. 66 Abs. 2 GTG.
[151] Art. 66 Abs. 3 GTG.
[152] Art. 67 GTG.
[153] Art. 71 GTG.

Verarbeitung und Nutzung von Proben menschlichen Materials (genetische Daten) in Biobanken regelt[154]. Daneben wurde eine Rechtsgrundlage für die Gesundheitsdatenbank erlassen: The Health Sector Database Act (HSDA)[155], das durch die Government Regulation on a Health Sector Database No 32/2000 konkretisiert worden ist. Dieses Gesetz sieht eine bevölkerungsweite, umfassende und allgemeine Erhebung von medizinischen und persönlichen Daten vor. Gesetzlich festgelegt ist, dass Kliniken und Ärzte umfängliche medizinische Daten erheben und erfassen und an eine zentrale Datenbank weitergeben. Die Zustimmung der Betroffenen ist nicht erforderlich, sie können lediglich der Aufnahme ihrer Daten in die Datenbank widersprechen[156]. Das Gesetz sieht dabei eine exklusive Nutzung der Datenbank durch die US-Firma deCODE zusammen mit der isländischen Tochter *Islensk erfdagreining* als Lizenznehmer für 12 Jahre vor.

Darüber hinaus autorisiert das Gesetz deCODE, die Datenbank mit zwei weiteren Datensammlungen zusammenführen[157]. Zum einen existiert in Island eine umfangreiche Sammlung an Gewebeproben. Seit 50 Jahren werden Proben, die bei einer medizinischen Behandlung oder der Untersuchung von Leichen gewonnen werden, in einer Gewebebank aufbewahrt[158]. Hinzu kommt eine medizinische Datensammlung, in der die seit 1915 geführten Patientenakten von allen Einwohnerinnen und Einwohnern erfasst sind[159]. Diese drei Datensammlungen bilden die Grundlage dieser bisher einzigartigen Gesundheitsdatenbank. Des Weiteren hatte deCODE bereits in einer genealogischen Datenbank die kompletten Stammbäume sämtlicher lebenden Isländerinnen und Isländer sowie einer großen Anzahl ihrer Vorfahren erfasst. Die Firma deCODE hat bis Ende 2002 krankheitsbezogene genetische Daten von ca. 110.000 Isländern aus einer Gesamtbevölkerung von 290.000 gesammelt und sie mit den o.g. gesundheits- und genealogischen Daten verknüpft.

In der Praxis waren allerdings viele Ärzte und Kliniken nicht bereit, Patientendaten weiterzugeben[160]. Im März 2003 entschied das isländische Verfassungsgericht, dass das Gesetz zur Datenbank nicht verfassungskonform ist, insbesondere weil der Schutz der Privatsphäre nicht gewährleistet sei und keine Vorschriften erlassen wurden, wie dieses Ziel zu erreichen ist[161]. Zudem monierte das Gericht die unzureichende Verschlüsselung der Daten bei einer so kleinen Population wie der Isländischen[162]. Damit war der Aufbau der Biobank gestoppt. Die Firma DeCODE änderte daraufhin ihre Geschäftsstrategie. Der Schwerpunkt wurde auf die Produktseite, d. h. die Identifizierung geeigneter Medikamente sowie ihre klinische Prüfung verlegt. Zwischenzeitliche Bestrebungen, einen verfassungskonformen Entwurf in das Parlament einzubringen, sind bisher nicht umgesetzt worden.

---

[154] Art 2 i. V. m. Art 3 AoB.
[155] Act on a Health Sector Database (HSD), abrufbar unter: http://eng.heilbrigdisraduneyti.is/laws-and-regulations/nr/659#allt
[156] Art 8 HDS.
[157] Art 10 HDS.
[158] TAZ 28.3 1998 „Ausverkauf mit Gewinnbeteiligung".
[159] Sokol, Gesundheitsdatenbanken und Betroffenenrechte: Das Isländische Beispiel, NJW 2002, 1767.
[160] Revermann/Sauter, Biobanken als Ressource der Humanmedizin, S. 90.
[161] The Icelandic Data Protection Authority: Judgment on the Health Sector Database, abrufbar unter http://www.personuvernd.is/information-in-english/greinar//nr/448.
[162] Revermann, Sauter S. 90.

3.2.2.4 Deutschland

3.2.2.4.1 Begriffsbestimmungen

3.2.2.4.1.1 Treuhänderschaft im Allgemeinen

Die Treuhänderschaft ist ein im Zivilrecht anerkanntes Rechtsinstitut. Die Übernahme von Treuhandaufträgen gehört z. B. zum Kernbereich der notariellen Tätigkeit. Insbesondere bei der Abwicklung von Grundstückskaufverträgen wird der Notar als Treuhänder eingeschaltet, sei es, dass der Kaufpreis über ein Notaranderkonto abgewickelt wird und erst an den Verkäufer gelangt, wenn lastenfreie Eigentumsübertragung gewährleistet ist, oder dass die Abwicklung im Wege der sogenannten Stufenlösung oder Direktzahlung vorgenommen wird, indem die zentrale Steuerung durch den Notar über die Fälligkeitsmitteilung erfolgt[163]. Eine Treuhandtätigkeit gegenüber mehreren Personen mit entgegengesetzten Interessen wird dabei als mehrseitige Treuhand bezeichnet[164]. In jedem Fall handelt es sich bei seinen treuhänderischen Tätigkeiten darum, dass dem Notar Rechtsmacht übertragen wird, die er gemäß einer von den Beteiligten gemeinsam erteilten Treuhandanweisung einzusetzen hat[165]. Ist der Treuhänder in Interessenkonflikten befangen, wie dies bei mehrseitiger Treuhand der Fall sein kann, bildet die in § 666 BGB geregelte Benachrichtigungspflicht eine besondere Ausprägung der treuhänderischen Interessenwahrnehmungspflicht: Hier ist der Treuhänder dem Treugeber (gegen den Wortlaut von § 666 BGB) stets **unaufgefordert** benachrichtigungspflichtig. Gleiches gilt außer für solchermaßen „konfliktbefangene“ Treuhänder auch für „Kompetenztreuhänder“, die sich auf Grund ihres Wissens oder ihrer Stellung gegenüber dem Treugeber in einem besonderen Kompetenzvorsprung befinden.[166] Kurz gefasst: Gegenüber dem Treugeber durch Kompetenz überlegene oder in Interessenkonflikten befangene Treuhänder müssen dem Treugeber in proaktiver Weise Transparenz gewähren.

3.2.2.4.1.2 Treuhänderschaft zum Zweck des Datenschutzes in der Forschung

In der Forschung spielt der Einsatz eines Treuhänders als Bestandteil eines umfassenden Datenschutzkonzepts insbesondere bei sehr sensitiven bzw. umfangreichen Datenbeständen eine wesentliche Rolle. Mit dem Einsatz von Datentreuhändern kann der Schutz der personenbezogenen Daten gewährleistet und der Eingriff in die Rechte der Betroffenen minimiert werden, ohne dass der Datenbedarf der Forschung behindert wird. Ein Treuhänder wurde in diesem Zusammenhang allgemein verstanden als rechtlich selbständiger, unabhängiger, vertrauenswürdiger Dritter, der zwischen die Daten besitzende Stelle und den Forscher bzw. zwischen den Betroffenen und den Forscher tritt. Datentreuhänder sind eigenständige Personen oder Einrichtungen, die zur Absicherung ihrer Treuhänderfunktion sowohl gegenüber der Daten besitzenden Stelle als auch gegenüber dem Forscher personell und räumlich klar getrennt sein müssen. Sie sollten weisungsunabhängig sein und sich auf ein Aussageverweigerungsrecht und ein entsprechendes Verbot der Beschlagnahme von Unterlagen stützen können – wie etwa Notare[167]. Gesetzliche Regelungen, die die

[163] Kemp, RNotZ 2004, 460.
[164] Reithmann in Schippel/Bracker, Bundesnotarordnung, zu § 24 Rn. 40.
[165] Reithmann in Schippel/Bracker, Bundesnotarordnung, zu § 24 Rn. 41.
[166] Löhnig, Treuhand – Interessenwahrnehmung und Interessenkonflikte, Tübingen, 2006, S. 834 f.
[167] Metschke, Wellbrock, Datenschutz in Wissenschaft und Forschung, 3. Auflage 2002, S. 43.

Vertrauenswürdigkeit eines Datentreuhänders explizit absichern, fehlen bislang. Dagegen sind sog. Vertrauensstellen eingerichtet bzw. gesetzlich vorgesehen worden, die eine entsprechende Funktion haben, z. B. nach den Krebsregistergesetzen der Länder und in der Gesetzlichen Krankenversicherung (SGB V). Gegenüber dem Betroffenen sowie der Daten besitzenden Behörde muss rechtlich und technisch-organisatorisch gewährleistet werden, dass nur der Datentreuhänder einen Personenbezug herstellen kann, die ihm von der Daten besitzenden Stelle oder vom Betroffenen selbst übermittelt worden sind. Nach der durch den Datentreuhänder erfolgenden Anonymisierung/Pseudonymisierung sollten die zu verarbeitenden eigentlichen Forschungsdaten nicht beim Datentreuhänder aufbewahrt werden, sondern lediglich die Identifikationsdaten und Verschlüsselungsalgorithmen.

Für die Übermittlung personenbezogener Daten an einen Datentreuhänder gelten die rechtlichen Vorgaben der Forschungsregelungen. Trotz seiner Funktion als unbeteiligter Dritter bedeutet die Übermittlung personenbezogener Daten an den Datentreuhänder einen Eingriff in das Selbstbestimmungsrecht der Betroffenen, das einer gesetzlichen Grundlage bedarf, soweit die Betroffenen nicht eingewilligt haben. Auf eine gesetzliche Grundlage kann nur in den Fällen verzichtet werden, in denen der Datentreuhänder die betreffenden Daten „blind“, z. B. durch Verschlüsselung unlesbar erhält und dennoch verknüpfen kann. Grundsätzlich muss daher die Biobank auf der Grundlage einer informierten Einwilligung der Betroffenen den Datentreuhänder einschalten.

3.2.2.4.1.3 Aufgaben des klassischen Datentreuhänders zur Gewährleistung des Datenschutzes der Betroffenen

Als typische Aufgabe des Treuhänders wird die Anonymisierung bzw. Pseudonymisierung und die Verknüpfung und Datensicherung angesehen.[168] Bei einer Anonymisierung/Pseudonymisierung der Daten durch den Treuhänder wird dieser zwischen die Daten besitzende Stelle und den Forscher gestellt. Er anonymisiert oder pseudonymisiert die von der Daten besitzenden 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 der personenbezogenen Daten erhalten, eng begrenzt und die Datensicherheit kann effektiv gewährleistet werden.

Ein Treuhänder kann es auch übernehmen, verschiedenen Datensätze aus verschiedenen Quellen oder unterschiedlichen Zeitpunkten oder unter verschiedenen Pseudonymen verborgene Daten derselben Person personenbezogen zusammenzuführen, anschließend erneut zu anonymisieren oder zu pseudonymisieren und in dieser Form an die beteiligten Forscher übermitteln. Er kann auch mehrere unterschiedliche Dateien personenbezogen verknüpfen und ggf. nach bestimmten Kriterien vorauswerten oder später neue Daten den Einzeldatensätzen zuordnen (linking). Er sichert somit entstehende Persönlichkeits(teil)bilder nach außen ab.

3.2.2.4.1.4 Beispiel eines klassischen Datentreuhänders: Das Projekt QuaSi-Niere

[168] Bizer, Der Datentreuhänder, Lösungsmodell für den Datenzugang der Forschung, 392, 394.

Im Modellprojekt QuaSi-Niere wurde, um eine Interessenkollision zwischen den Trägern des Registers (Krankenkassen, Behandlungseinrichtungen und Patientenverband) auszuschließen und somit die Interessen der Betroffenen zu wahren, ein Notar mit der Datentreuhandschaft für das Patientenregister beauftragt. Er ist auf der Grundlage einer Verfahrensordnung eine selbständige, vertrauenswürdige, eigenverantwortliche und unabhängige Institution. Als eigenständige Daten besitzende Stelle ist er zuständig für die Entgegennahme, Pseudonymisierung, Re-Identifizierung und Weitergabe von (anonymen) Daten, die mit Einwilligung der Patienten erhoben und von den behandelnden Ärzten an ihn übermittelt werden. Ihm ist ein Beirat (ein nicht am Projekt beteiligter Arzt und ein Vertreter des Patientenverbandes) zur Seite gestellt. Beim Projekt QuaSi-Niere wird vom Datentreuhänder die Verknüpfungsfunktion wahrgenommen. Der Treuhänder erhält Daten desselben Patienten aus verschiedenen Einrichtungen und versieht sie mit einem identischen Pseudonym, so dass sie im Register verknüpft werden können. Auch die Behandlungseinrichtung wird pseudonymisiert[169].

3.2.2.4.1.5 Neue Entwicklungen

In neuerer Zeit wird ein Einsatz von Treuhändern darüber hinausgehend auch im Zusammenhang mit wesentlich umfassenderen, komplexeren Aufgabenwahrnehmungen thematisiert, z. B. als Anbieter von technischem Service. Dementsprechend werden auch hohe Anforderungen an die technische und rechtliche Kompetenz des Treuhänders und auch an seine Ressourcen gestellt. Daneben ist sein Einsatz auch als Informationsberater für die von der Datenverarbeitung durch mehrere Stellen Betroffenen sowie als Garant der Einhaltung der Anforderungen an eine informierte Einwilligung denkbar. Man könnte dann von einer materiellen Datentreuhänderschaft sprechen, wenn es um die Einhaltung der Anforderungen an die Einwilligung und Aufklärung der Spender geht – und von einer formellen Datentreuhänderschaft, wenn es um die klassischen Aufgaben des Datentreuhänders durch seine Zwischenschaltung für Zwecke der Sicherstellung der Vertraulichkeit geht, d. h. wenn es bildlich gesprochen um die Verwahrung des Schlüssels zu den personenbezogenen Daten geht. Diese Unterscheidung in den Begrifflichkeiten ist bisher kaum gebräuchlich, dient aber der Verdeutlichung der unterschiedlichen Aufgaben des Treuhänders.

Weiter ist das Modell eines „elektronischen“ Datentreuhänders entwickelt worden. Darunter wird im Wesentlichen ein Treuhänder verstanden, der eine zentrale Patientenliste elektronisch verwaltet. Der Treuhänder erhält die den Spender / die Betroffenen identifizierenden Daten elektronisch übermittelt und übermittelt umgehend ein Pseudonym zurück. Alle Daten, die im Verlauf der Studie von verschiedenen Ärzten und Forschern ermittelt werden, werden unter der Verwendung des Pseudonyms verwaltet. Eine möglicherweise notwendige Depseudonymisierung kann ausschließlich von autorisierten Personen nach einem strengen Regelwerk durchgeführt werden.[170]

3.2.2.4.2 Datentreuhänderschaft im deutschen Recht

Die Institution des Datentreuhänders bzw. Institutionen, die entsprechenden Zwecken dient, sind im deutschen Recht vereinzelt gesetzlich erwähnt, jedoch nicht umfassend geregelt. Das BDSG sowie die

[169] Vgl. dazu Metschke, Wellbrock, Datenschutz in Wissenschaft und Forschung, 3. Auflage 2002, S. 43f., 17. Tätigkeitsbericht des Bayrischen Landesbeauftragten für den Datenschutz, 1996, S. 34f.
[170] TMF, Rechtsgutachten zur elektronischen Datentreuhänderschaft, S. 13.

Landesdatenschutzgesetze enthalten jeweils allgemeine Forschungsklauseln, in denen bestimmt ist, dass die Merkmale gesondert zu speichern sind, mit denen Einzelangaben einer bestimmten oder bestimmbaren Person zugeordnet werden können, sobald oder soweit der Forschungszweck dies zulässt[171]. Am 24. April 2009 hat der Bundestag das von der Koalition vorgelegte Gendiagnostikgesetz verabschiedet, das jedoch weder Regelungen zur Forschung mit genetischen Daten noch zur Datentreuhänderschaft enthält. Vereinzelte Erwähnung finden die (Daten-)Treuhänderschaft bzw. ähnlich gelagerte Institutionen im Transplantationsgesetz (TPG), im Transfusionsgesetz (TFG), im 5. Sozialgesetzbuch (Gesetzliche Krankenversicherung – SGB V), in den Krebsregistergesetzen der Länder sowie im Hamburgischen Krankenhausgesetz (HambKHG), das als einziges Land Sonderregelungen für Biobanken erlassen hat.

3.2.2.4.2.1 Gendiagnostikgesetz

Das vom Bundestag verabschiedete Gendiagnostikgesetz (GenDG) enthält Vorschriften zu genetische Untersuchungen zu medizinischen Zwecken, zu genetischen Untersuchungen zur Klärung der Abstammung sowie zu genetischen Untersuchungen im Versicherungsbereich und im Arbeitsleben. Nach § 18 des Gesetzes darf der Arbeitgeber von Beschäftigten weder vor noch nach Begründung des Beschäftigungsverhältnisses die Vornahme genetischer Untersuchungen oder Analysen verlangen oder die Mitteilung von Ergebnissen bereits vorgenommener genetischer Untersuchungen oder Analysen verlangen, solche Ergebnisse entgegennehmen oder verwenden. Auch Versicherungsunternehmen dürfen grundsätzlich keine Auskünfte über genetische Daten verlangen. Ausgenommen sind Lebens-, Berufsunfähigkeits-, Erwerbsunfähigkeits- oder Pflegerentenversicherungen mit einer Leistung von mehr als 300.000 Euro insgesamt oder 30.000 jährlich. Regelungen zur Forschung mit genetischen Daten oder zur Datentreuhänderschaft sind in dem Gesetz nicht enthalten[172].

3.2.2.4.2.2 Transplantationsrecht – Transfusionsrecht

Das TPG betrifft die Organspende verstorbener oder lebender Personen[173]. Die vermittlungspflichtigen Organe dürfen nur in besonderen Transplantationszentren verpflanzt werden, nachdem die gesetzlich eingerichtete Vermittlungsstelle sie dorthin vermittelt hat[174]. Es gelten dabei Regeln, die materiell Strukturen von Datentreuhänderschaft festlegen, indem sie die von der Vermittlungsstelle getrennte Koordinierungsstelle einführen. Ihre Aufgabe ist die Entnahme des Spenderorgans und die Verschlüsselung der personenbezogenen Daten des Spenders[175]. Diese spenderschützenden Aufgaben nimmt sie wahr, indem sie die personenbezogenen Daten des Spenders in einer Weise verschlüsselt, die nur ihr (und nicht der Vermittlungsstelle) den Rückschluss auf die Person des Spenders erlaubt.

---

[171] Vgl. § 40 BDSG, § 33 HDSG, § 28 DSG NRW, § 30 BlnDSG, § 35 LDSG Baden-Württemberg, Art. 23 BayDSG, §28 Bbgdsg, § 19 BremDSG, § 27 HambDSG, § 34 DSG-MV, § 25 NDSG, § 30 SDSG Rheinland-Pfalz, § 30 SDSG, § 27 DSG-LSA, § 25 ThürDSG, § 36 SächsDSG. Das LDSG SH hat keine entsprechende ausdrückliche Bestimmung

[172] Der Entwurf eines Gesetzes über genetische Untersuchungen bei Menschen (Gendiagnostikgesetz – GenDG), Drucksache 16/ 10532 ist abrufbar unter: http://dip21.bundestag.de/dip21/btd/16/105/1610532.pdf. BGBl.

[173] §§ 3 und 8 TPG.

[174] §§ 10 und 11 TPG:

[175] §§ 11 und 13 TPG.

Ähnliche Regeln finden sich im TFG für Blutspenden[176], in dem u. a. die Einrichtung eines Hämophilieregisters festgelegt ist, das als Bundesoberbehörde geführt wird[177]. Die Haltung der die Patienten identifizierenden Daten erfolgt dezentral beim behandelnden Arzt, der nur eine Patientennummer an das Hämophilieregister übermittelt. Diese Nummer wird in eine zweite Nummer umgesetzt. Der Zusammenhang von Patientennummer und Patientenpseudonym wird von einem Intermediär – einer zwischengeschalteten Einrichtung datenschutzfördender Technik (im Ergebnis ist dies ein spezieller Server) – verwaltet[178].

3.2.2.4.2.3 SGB V (Gesetzliche Krankenversicherung – GKV)

Die §§ 303 ff SGB V sehen eine Zusammenführung der Leistungs- und Abrechnungsdaten aller Versicherten in einem zentralen Datenpool vor, damit eine valide Datenbasis geschaffen werden kann für eine zielgerichtete Systemsteuerung der GKV durch die Selbstverwaltung und die Politik auf Bundes- und Landesebene. Dazu sollen eine Vertrauensstelle und eine Datenaufbereitungsstelle eingerichtet werden. Durch die Datenaufbereitungsstelle sollen die übermittelten Daten zusammengeführt und anschließend aufbereitet werden. Die Vertrauensstelle hat die ihr übermittelten personenbezogenen Daten durch ein gesetzlich vorgeschriebenes Verfahren zu pseudonymisieren. Die bei der Datenaufbereitungsstelle gespeicherten Daten können von zahlreichen, im Gesetz abschließend festgelegten Stellen verarbeitet und genutzt werden, soweit dies für die Erfüllung ihrer Aufgaben erforderlich sind.[179]

3.2.2.4.2.4 Krebsregistergesetze der Länder

In den Krebsregistergesetzen der Länder, die zur Verbesserung der Datengrundlage für die Krebsepidemiologie erlassen worden sind, finden sich Regelungen über Vertrauensstellen. Auch diese Vertrauensstellen sind in ihrer Funktion und Aufgaben mit einem Datentreuhänder vergleichbar.

Im Krebsregistergesetz für Schleswig-Holstein (LKRG) wird zwischen Identitätsdaten und epidemiologischen Daten unterschieden[180]. Das Krebsregister besteht dabei aus der bei der Ärztekammer Schleswig-Holstein unter ärztlicher Leitung geführten Vertrauensstelle und der beim Institut für Krebsepidemiologie e.V. in Lübeck eingerichteten Registerstelle[181]. Die Vertrauensstelle

- nimmt von den Ärzten bzw. den Kreisen und kreisfreien Städten namentlich zu machende Meldungen über Krebserkrankungen entgegen[182].
- Sie prüft die ihr übermittelten Daten auf Schlüssigkeit und Vollständigkeit und übermittelt dann die epidemiologischen Daten einschließlich einer von ihr vergebenen Patientennummer an die Registerstelle[183].

---

[176] §§ 1 und 21 TFG.
[177] § 21 TFG.
[178] Vgl. dazu ausführlich unter: http://www.pei.de/cln_047/nn_474366/SharedDocs/Downloads/blut/dhr/02dhr-konzept-ergaenzung,templateId=raw,property=publicationFile.pdf/02dhr-konzept-ergaenzung.pdf.
[179] § 303f Abs. 1 SGB V.
[180] § 3 Abs. 1 und 5 LKRG.
[181] § 2 Abs. 2 und 3 LKRG.
[182] § 4 Abs. 1 und 7 LKRG.
[183] § 6 Abs. 4 LKRG.

- Nach einer Wartefrist löscht sie die Identitätsdaten des Betroffenen, wenn ihr keine Einwilligung des Betroffenen in die Forschungsverwendung seiner Daten vorliegt. [184]
- Die Registerstelle erhält keine personenbezogenen Daten.
- Die Zusammenführung von Daten zur Erkrankung mit Daten zur Person ist über die Vertrauensstelle nur in den gesetzlich vorgesehen Fällen zulässig. Dazu bestimmt § 9 LKRG:

  (1) Die Landesregisterbehörde kann auf Antrag die Zusammenführung personenbezogener und epidemiologischer Daten genehmigen, wenn dies für die Durchführung wichtiger und im öffentlichen Interesse liegender Forschungsvorhaben erforderlich ist. Der Antrag ist zu begründen. Ihm ist eine Stellungnahme einer Ethikkommission oder eines Beirates eines Krebsregisters beizufügen, wenn eine solche für das Forschungsvorhaben vorgeschrieben oder eingeholt worden ist.

  (2) Wird der Antrag nach Absatz 1 genehmigt, ermittelt die Vertrauensstelle Familiennamen, Vornamen und Anschrift der Personen, die die Zustimmung zur Mitwirkung an Forschungsvorhaben oder eine Zustimmung nach § 4 Abs. 4 des Landeskrebsregistergesetzes (…) erteilt haben und führt diese Daten mit den von der Registerstelle zu übermittelnden epidemiologischen Daten vorübergehend zusammen. Die Daten sind der Antragstellerin oder dem Antragsteller in dem erforderlichen Umfang zur Verfügung zu stellen, wenn sie oder er sich verpflichtet, die Verarbeitung der Daten durch das Unabhängige Landeszentrum für Datenschutz nach § 41 des Landesdatenschutzgesetzes kontrollieren zu lassen und die hierfür entstehenden Kosten zu tragen. (…)

  (3) Die Vertrauensstelle hat in der Übermittlung nach Absatz 2
  1. die Empfängerin oder den Empfänger der Daten sowie die für das Vorhaben verantwortliche Person,
  2. das Vorhaben, zu dem die übermittelten personenbezogenen Daten ausschließlich verwendet werden dürfen, und
  3. den Tag, bis zu dem die übermittelten Daten aufbewahrt werden dürfen, zu bestimmen. Beträgt die Frist nach Nummer 3 mehr als zwei Jahre, sind die Patientinnen oder Patienten von der Vertrauensstelle entsprechend zu informieren. Die Übermittlung der Daten an die Empfängerin oder den Empfänger kann auch nachträglich mit Nebenbestimmungen versehen werden.

  (4) Die Empfängerin oder der Empfänger der Daten darf die übermittelten Daten nicht an Dritte weiterübermitteln. Sie oder er hat der Landesregisterbehörde jede Veränderung von Umständen unverzüglich anzuzeigen, die für die Entscheidung über den Antrag wesentlich waren. Bei Fortfall der Voraussetzungen für die Übermittlung entscheidet die Landesregisterbehörde, ob die Empfängerin oder der Empfänger die Daten zu löschen oder an die Vertrauensstelle zurückzugeben hat. Die danach sowie die nach Absatz 3 Nr. 3 erforderliche Löschung der gespeicherten Daten ist der Vertrauensstelle anzuzeigen.

[184] § 6 Abs. 2, Abs. 4 und 5 LKRG.

3.2.2.4.2.5 Das Biobankrecht des Hamburgischen Krankenhausgesetzes

Die Freie und Hansestadt Hamburg hat 2006 Regelungen zum Spenderschutz sowie zur Datentreuhänderschaft in das Hamburger Landeskrankenhausgesetz (HmbKHG) aufgenommen. In § 12a HmbKHG heißt es:

§ 12a Sammlungen von Proben und Daten

(1) Das Sammeln von Proben und Patientendaten zu allgemeinen Forschungszwecken ist zulässig, wenn die betroffenen Personen über Zweck und Nutzungsmöglichkeiten der Sammlung aufgeklärt wurden und in die Probenentnahme und Datenerhebung sowie in die Aufnahme von Proben und Daten in die Sammlung eingewilligt haben. Satz 1 gilt entsprechend für die Übernahme bereits vorhandener Proben und Daten. Einer besonderen Einwilligung bedarf es nicht, wenn die behandelnde Krankenhauseinheit die zu Behandlungszwecken aufbewahrten Proben und gespeicherten Daten vor der Weitergabe zur Sammlung anonymisiert. Dies gilt auch für Proben, die bei klinischen und rechtsmedizinischen Sektionen entnommen wurden.

(2) Erfordert der Zweck der Sammlung die Möglichkeit einer Zuordnung, sind die Proben und Daten vor der Aufnahme in die Sammlung zu pseudonymisieren.

(3) Vor einer Weitergabe von Proben und der Übermittlung von Daten für bestimmte Forschungsvorhaben nach § 12 ist die Möglichkeit der Zuordnung zur betroffenen Person aufzuheben oder, wenn der Forschungszweck dem entgegensteht, eine weitere Pseudonymisierung vorzunehmen.

(4) 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.

(5) Die Einrichtung von Proben- und Datensammlungen zu allgemeinen Forschungszwecken ist der für die Datenschutzkontrolle zuständigen Behörde anzuzeigen. Die Anzeige ist jeweils nach fünf Jahren mit einer Begründung für die weitere Speicherung zu erneuern.

Im Wesentlichen stellt die Vorschrift, die für krankenhausinterne Biobanken gilt, klar, dass die Einholung einer Einwilligung erforderlich ist bzw. die Daten und Proben zu anonymisieren sind. Erfolgt auf der Grundlage einer Einwilligung keine Anonymisierung der Daten und Proben, sind diese vor Aufnahme in die Biobank zu pseudonymisieren – ggf. durch einen externen Datentreuhänder. Neue Biobanken in Hamburger Krankenhäusern sind beim Hamburgischen Datenschutzbeauftragten anzuzeigen.

3.2.2.4.2.6 Spezifische Anforderungen an vertrauenswürdige Biobanken

Konsens besteht darüber, dass die bestehende Rechtslage unbefriedigend ist und zusätzlich zu den allgemeinen Wirksamkeitsvoraussetzungen einer datenschutzrechtlichen Einwilligung („informed consent“, vgl. § 4a BDSG) weitere Zulässigkeitsbedingungen bestehen müssen, um den Betroffenen

vor Zwangslagen und unbedachten existenziellen Erklärungen zu schützen. Entsprechend den existierenden Regelungen insbesondere zu den Vertrauensstellen im medizinischen Bereich sind spezifische Forderungen an Biobanken auch in Deutschland aufgestellt worden[185]. Diese sind zwar nicht gesetzlich fixiert, sind jedoch erforderlich, um einen ausreichenden Schutz des informationellen Selbstbestimmungsrechts zu gewährleisten.

Anforderung an die Einwilligung einer Biobank

Die Umsetzung der Anforderungen an eine rechtswirksame Einwilligung ist in mehrfacher Hinsicht wegen der dargestellten Besonderheiten bei der Biobank-Forschung problematisch: Biobanken erheben Spenderdaten für wechselnde Forschungsprojekte, so dass weder der Zweck der Datenverarbeitung vollständig konkretisiert werden kann, noch die Empfänger abschließend benannt werden können und sich schließlich der Informationsgehalt der Spenderdaten im Hinblick auf die zunehmenden Möglichkeiten der genetischen Analysen erhöhen kann und wird. Um dennoch eine rechtswirksame Einwilligung zu erreichen, müssen ausgleichende Maßnahmen getroffen werden. Zum einen müssen eine Ausschlussmöglichkeit der Forschungszwecke und eine Abstufung des Einwilligungsumfangs und des Einwilligungszweckes möglich sein bzw. vorgenommen werden. Hinsichtlich der Forschungserträge muss dem Spender eine Wahloption eingeräumt werden. Weiter muss eine entsprechend angepasste Information und Aufklärung der Betroffenen stattfinden und eine Standardisierung der Einwilligung vorgenommen werden:

- Die Spenderin bzw. der Spender muss bei der Abgabe des Materials und der Daten bei der Biobank in der Einwilligung die Möglichkeit erhalten, bestimmte Forschungszwecke, Geldgeber und Kooperationspartner allgemein auszuschließen.
- Es müssen Abstufungen des Einwilligungsumfangs und des Einwilligungszwecks ermöglicht werden. Es muss für alle Biobanken, die ihre Spender nicht für einzelne bestimmte Forschungsprojekte derselben Art aussuchen, verpflichtend gemacht werden, dem Spender Auswahloptionen wegen des Umfangs der von ihm erteilten Einwilligung einzuräumen.
- Häufig ist es für den Spender wichtig, über Forschungsergebnisse zu erfahren, die mit Hilfe seiner Daten und Proben erzielt wurden und die sich abstrakt auch auf seine eigene gesundheitliche Situation beziehen können („donor feedback“). Dem Spender muss daher schon in der Spendereinwilligung die Möglichkeit eingeräumt werden, entsprechende Informationen über Forschungserträge zu beziehen. Zur Erleichterung für die Spender muss es sich dabei um ein Push-Verfahren handeln, bei dem dem Spender die fraglichen Informationen an eine von ihm benannte Adresse geliefert werden.
- Die der Einwilligung vorhergehende Aufklärung hat mündlich und schriftlich zu erfolgen.
- Die Biobank hat mindestens über Folgendes aufzuklären:
  - Freiwilligkeit der Teilnahme,
  - Zwecke, Art, Umfang und Dauer der vorgesehenen Nutzung einschließlich vorgesehener genetischer Analysen,

---

[185] u. a. Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) zum Entwurf der Bundestagsfraktion Bündnis 90/Die Grünen eines Gendiagnostikgesetzes vom 3.11.2006 (BT-Drs. 16/3233) zur Anhörung am 7.11.2007, abrufbar unter https://www.datenschutzzentrum.de/medizin/genom/20071107-gendiagnostikgesetz.pdf; Der Hamburgische Datenschutzbeauftragte, Anforderungen an Biobanken, abrufbar unter http://www.hamburg.de/gesundheit-soziales/233648/bio-banken.html.

  - Umfang und Bedingungen einer möglichen Weitergabe von Proben und Daten,
  - Verfahren der Rückmeldung von Forschungsergebnissen an den Spender,
  - Hinweise auf mögliche Konsequenzen der Mitteilung von Befunden genetischer Analysen für den Spender und verwandte Angehörige einschließlich möglicher Offenbarungspflichten (z. B. gegenüber Versicherungen),
  - Art der Speicherung und Zusammenführung von Daten,
  - Anonymisierung oder Pseudonymisierung von Proben und Daten, und sonstige flankierende Maßnahmen des Spenderschutzes,
  - etwaige staatliche Zugriffsmöglichkeiten auf Proben und Daten,
  - das Recht des Spenders auf jederzeitigen Widerruf seiner Einwilligung ohne Sanktionen,
  - das Schicksal von Proben und Daten beim Widerruf und bei Beendigung der Biobank,
  - etwaige kommerzielle Perspektiven der vorgesehenen Forschung und Fragen der Aufwandsentschädigung, Bezahlung,
  - Ziele der Forschung,
  - Herkunft der Finanzmittel,
  - vorgesehenen Kooperationspartner.
- Der Spender muss zur Vertiefung nachlesen können, was ihm mündlich erklärt wurde.
- Dem Spender muss wegen seiner Entscheidung eine Bedenkzeit eingeräumt werden.
- Der Spender muss nicht nur im Zeitpunkt der Einwilligung, sondern laufend über die Biobank und die Verwendung bzw. Verarbeitung seiner Daten informiert werden. Ausführlich dazu unter 4.5.

Zweckbindung

Je abstrakter und umfassender der Forschungszweck, desto höhere Anforderungen sind an die fortwährende Information der Spender zu stellen (dazu unter 4.5).

Erforderlichkeit und Datensparsamkeit

- Biobanken haben eine frühestmögliche Pseudonymisierung und Anonymisierung vorzusehen sowie den Zeitpunkt der Löschung vorzusehen. Dafür sind Lösch- und Prüffristen vorzusehen.
- Angesichts der möglichen neuen Erkenntnisse ist dabei nicht nur die Erforderlichkeit zu überprüfen, sondern auch, ob bei anonymisierten Daten weiterhin die Anonymität gewährleistet ist.
- Bei personenbezogenen oder pseudonymisierten Daten muss gewährleistet sein, dass ein nachträglicher Widerspruch (Rücknahme der Einwilligung) zur Datenlöschung führt.
- Eine Einwilligung in eine unbefristete nicht wenigstens pseudonymisierte Aufbewahrung ist unzulässig.

Betroffenenrechte

Außerdem sind die Betroffenenrechte, insbesondere das Auskunftsrecht des Betroffenen über seine Daten, ihre Herkunft und Empfänger sowie seine Berichtigungs- und Löschungsansprüche zu gewährleisten. Folgende Forderungen sind zu erfüllen:

- Eine Biobank soll die Rückmeldung personenbeziehbarer Diagnosen und Forschungsfunde an den Spender nicht ausschließen. Eine Biobank, die Rückmeldungen an den Spender von

Anfang an generell ausschließt, begibt sich in den Verdacht, Biomaterial in einer möglichst marktgängigen Form (ohne die Belastung mit dem Rückmeldungsrisiko) im Angebot haben zu wollen, losgelöst davon, ob ein Ethikvotum zu einem Projekt – z. B. des Jahres 2017 – eine solche Rückmeldung vielleicht anordnen wird.

- Das Recht auf Widerruf ist unabdingbar.
- Das Widerrufsrecht der Spender muss bei jeder Weitergabe von Proben und Daten gewährleistet sein.
- Damit dieses Widerrufsrecht in der Praxis auch durchgesetzt werden kann, sollte jede Weitergabe an Dritte nachvollziehbar dokumentiert werden, damit gewährleistet ist, dass größtmögliche Transparenz herrscht und die Spender ihre Proben und Daten jederzeit zurückziehen können.

3.2.3 Ergebnis des Rechtsvergleichs

Der Rechtsvergleich hat ergeben, dass die Regelungstiefe in den verschiedenen Ländern Biobanken betreffend sehr unterschiedlich ist. Auch die Verbindlichkeit der Regelungen ist sehr unterschiedlich, sie reicht von Empfehlungen bis hin zu gesetzlich angeordneten Vorgaben.

Allgemein anerkannt ist Folgendes:

- Daten und Proben in Biobanken müssen durch angemessene technische und organisatorische Maßnahmen vor missbräuchlicher Verwendung wirksam geschützt werden.
- Insbesondere muss eine Trennung zwischen den die Betroffenen identifizierenden Daten und den Daten und Proben erfolgen.
- Es sind klare Zugangs- und Nutzungsregeln festzulegen.
- Anonymisierung oder Pseudonymisierung der Daten des Betroffenen sind unerlässlich.
- Zum Schutz des Spenders sollte die Kodierung der Proben so früh wie möglich, spätestens aber bei Aufnahme in die Biobank erfolgen.

Des Weiteren haben sind die folgenden Maßnahmen mehrfach als Empfehlung ergangen oder bereits gesetzlich verankert worden, so dass diese als Grundsätze für eine gute Biobank-Praxis bzw. als Vorgabe für eine gesetzliche Regelung herangezogen werden können.

Zu besonderen Schutzmaßnahmen insb. durch Dritte:

- Es bedarf externer Kontrollen etwa durch eine unabhängige Aufsicht (Datenschutzbehörde / Ethikkomittees / Kontrollkomittee); möglichst vor Errichtung der Biobank.
- Eine Aufklärung über die Risiken sollte ggf. von einem Arzt durchgeführt werden.
- Zur betrieblichen Sicherstellung der Wirksamkeit von spenderschützenden Maßnahmen muss ein unabhängiger Dritter eingeschaltet werden, der unter besonderer Schweigepflicht stehen sollte. Die Verletzung dieser Pflicht sollte strafbewehrt sein.
- Der Schlüssel zu den personenbezogenen Daten soll von einer unabhängigen Stelle aufbewahrt werden, die nicht direkt an der Forschung mit den Proben und Daten der Biobank beteiligt ist.

Zur Datenübermittlungen an Dritte:

- Proben von menschlichem biologischem Material dürfen nur in anonymisierter Form weitergeleitet werden.
- Jede Weitergabe muss nachvollziehbar dokumentiert und in einem Transfervertrag (Material Transfer Agreement, MTA) geregelt werden.
- Datenübermittlungen aus Biobanken an Dritte müssen auf bestimmte konkret definiert Empfänger und konkret bezeichnete Forschungsvorhaben beschränkt sein, die von der übermittelnden Biobank darauf zu verpflichten sind, die Daten nur für den ursprünglichen Zweck zu verarbeiten, nicht an Dritte weiter zu übermitteln und diese nach Abschluss des Forschungsprojektes zu löschen.

Zu Dokumentations- / und Konkretisierungspflichten:

- Die Dokumentation der Biobank soll die Organisation, die Verantwortlichkeiten und den Anwendungsbereich der Biobank regeln. So muss z. B. festgelegt werden, wie die Aufsicht und Kontrolle über die Biobank organisiert sowie die Einhaltung des Qualitätsmanagements sichergestellt werden sollen.
- Sie soll Bestimmungen betreffend die Herkunft der aufbewahrten Proben, den Verwendungszweck sowie den Kreis der Zugangsberechtigten und den Voraussetzungen für den Zugang enthalten.
- Die Aufnahmekriterien, die Verwendung und die Aufbewahrungsdauer für die Biobank sind festzulegen. Darüber hinaus müssen Kriterien festgehalten werden, wie die biologischen Materialien und Personendaten genutzt und wie lange sie aufbewahrt werden sollen.
- Jede Probe sollte mit ihrer zugehörigen Einwilligung dokumentiert sein.

Zu Transparenz- und Informationspflichten:

- Biobanken sollten genehmigungs- bzw. anzeigepflichtig sein.
- Die Betroffenen sollten darüber informiert werden, wie Datenschutz und Vertraulichkeit gewährleistet werden. Die Information sollte gestuft erfolgen: in einfach verständlicher und zusammengefasster Form für alle und in einer zweiten Schicht mit allen Details und unter vollständiger Darstellung der Komplexität („layered privacy notice“).
- Die Betroffenen erhalten Informationen über die Speicherart und die Zusammenführung von Daten.
- Der Betroffene wird über die Konsequenzen von Erkenntnissen aus einem individuellen Feedback für seine Verwandtschaft informiert.
- Dem Betroffenen sollen die tatsächlichen und rechtlichen Grenzen des Schutzes sowie die Konsequenzen erklärt werden, die ein Bruch der Vertraulichkeit für ihn haben kann.
- Der Sammlungszweck und die Regeln über Vorhaltung, Nutzung und Weitergabe des Materials sollten spezifiziert und transparent sein. Sie sollten klar formuliert und so früh und breit kommuniziert werden, wie dies möglich ist, besonders, aber nicht ausschließlich, an mögliche Spender und Nutzer.
- Der Umfang sowie die Art und Dauer der Datenverarbeitung müssen transparent sein.
- Biobanken sollten über ihre zurückliegenden und ihre geplanten Vorhaben mindestens jährlich berichten inklusive vorgesehener genetischer Analysen.

- Die Finanzierung der Biobank sollte explizit und transparent gemacht werden.
- Wo die Möglichkeit besteht, dass eine Biobank privates oder ausländisches Kapital einwirbt oder mit der Verfolgung kommerzieller Interessen beginnt, sollte dies besonders den Spendern klar vermittelt werden.
- Die Biobank muss über staatliche Zugriffsrechte informieren sowie über ggf. gegebene Offenbarungspflichten (z. B. Versicherungen).
- Biobanken müssen bekannt machen, ob und wie sie Forschungserträge kommerzialisieren wollen.
- Es wird ein Register der Biobanken geführt, das über Internet zugänglich ist und von jeder Person einsehbar ist.
- Die Betroffenen müssen über ihre Rechte aufgeklärt werden.

Zu den Betroffenenrechten:

- Für Datenschutz und Schutz der Vertraulichkeit sollte in der Biobank eine verantwortliche Position identifiziert sein bzw. ein Datenschutzbeauftragter bestellt werden.
- Die Betroffenen haben das Recht, ohne Angabe von Gründen die Teilnahme an einem Forschungsprojekt zu verweigern.
- Ein schriftlicher Widerruf der Zustimmung zur Speicherung der Proben und Daten ist jederzeit möglich. In diesem Fall dürfen die Daten für neue Verwendungszwecke ab dem Zeitpunkt des Widerrufs nicht mehr herangezogen werden. Proben und Daten sind in der Biobank zu löschen.
- Es muss kommunizierte Regeln darüber geben, wann welche Informationen aus der Forschung zurück in die Biobank gehen und wann solche Informationen an den Spender weiterzuleiten sind.
- Die Rückkopplung ungesicherter Forschungserträge an Spender muss unterbleiben.
- Die Biobank muss die Verfolgbarkeit von Proben und Daten sicherstellen, damit sichergestellt ist, dass der Spender sein Recht ausüben kann, seine Einwilligung zurückzunehmen[186].
- Die Biobank muss sich unmissverständlich dazu erklären, ob und welche Rechte Spender an Proben und Daten zurückbehalten.
- Die Betroffenen haben das Recht, auf Informationen verzichten.
- Der Spender muss vor seiner Entscheidung über seine Spende ausreichend Bedenkzeit haben.

Zu Prozessmanagement und Qualitätssicherung und Audit:

- Es soll ein Qualitätsmanagement bzw. ein Datenschutzmanagement eingerichtet werden.
- Es sollten regelmäßige nicht anlassbezogene Audits (Prüfungen) durchgeführt werden, die den Zugang zu Proben und die Benutzung von Proben betreffen.
- Es sollten Prozeduren für die Übertragung der Biobank auf einen anderen Betreiber und für ihre Schließung entwickelt werden.
- Es werden Regelungen zur Einhaltung der Vorgaben der informierten Einwilligung verlangt.

[186] Diese Anforderung steht in einem Spannungsverhältnis zu einer möglichst frühzeitigen Anonymisierung.

- Die Biobank soll für ihre betrieblichen Prozesse Standard Operating Procedures (SOP) entwickeln bzw. soll zur Einhaltung seiner gesetzlichen Pflichten Protokolle und Prozesse vorhalten, die die Privatsphäre der Spender schützen.

Sonstige Maßnahmen, die als geeignet empfohlen werden:

- Die Entwicklung von Verhaltensregeln durch die „Gemeinschaft der Biobanken“ soll gefördert werden.
- Arbeitgebern und Versicherern ist es verboten, Ergebnisse von genetischen Analysen von ihren Arbeitnehmern, Arbeitsuchenden oder Versicherungsnehmern oder Versicherungswerbern zu erheben, zu verlangen, anzunehmen oder sonst zu verwerten.

3.3 Anwendung des klassischen deutschen Datentreuhändermodells auf Biobanken

Nach dem klassischen Datentreuhändermodell ist der Datentreuhänder eine eigenständig und weisungsfrei handelnde Stelle. Danach muss der Datentreuhänder die folgenden Voraussetzungen erfüllen:

- In der Person liegende Vertrauenswürdigkeiten (Schweigepflicht)
- Wirtschaftliche Unabhängigkeit
- Rechtliche Weisungsunabhängigkeit
- Keine Interessenkollision
- Unabhängigkeit in organisatorischer, technischer und räumlicher Sicht
- Technisch-organisatorische Ausstattung für die alleinige Beherrschung des Personenbezugs

Fraglich ist, ob dieses Konzept in der Biobanken-Forschung anwendbar ist, die zu einem großen Teil im privaten Bereich durchgeführt wird. Zunächst ist zweifelhaft, ob ein externer Datentreuhänder im privaten Geschäftsbereich von seinen Auftraggebern mit den notwendigen finanziellen Mitteln ausgestattet wird, um seine wirtschaftliche Unabhängigkeit zu gewährleisten. Des Weiteren darf diese Person kein Teilnehmer der Wertschöpfungskette sein, die ein Interesse an Existenz und Fortbestand der Biobank und an der wechselnden Beforschbarkeit von Proben und Daten hat. Außerhalb staatlicher Instanzen ist bloße rechtliche Selbständigkeit für ein Mehr an Vertrauenswürdigkeit nicht ausreichend. Der Datentreuhänder darf selbst nicht in der Forschung bzw. der Biobank tätig und darf der Biobank nicht ökonomisch oder durch sonstige Interessen verbunden sein. Eine feste Lieferbeziehung zwischen einem Krankenhaus, das in den Räumlichkeiten dieses Krankenhauses Daten und Proben von Patienten-Spendern einwirbt, würde demnach das Krankenhaus als Datentreuhänder disqualifizieren.

Außerdem ist fraglich, ob der Datentreuhänder über die entsprechende Probenhandhabungsinfrastruktur verfügen kann. Der externe für eine Biobank eingesetzte Datentreuhänder muss beim Austausch der Erhebungspseudonyme zu Daten und Proben den Bezug zwischen Proben und Daten (die Probe-Daten-Relation) aufrechterhalten und auch sie als Geheimnis beherrschen. Dem kann er nur gerecht werden, wenn er nicht nur mit den Daten, sondern auch mit den Proben umgeht.

Dieses Doppel-Erfordernis ist eine für Biobanken spezifische Besonderheit, die sich bei jedem „Tätigkeits-Abschnitt“ wiederholt: Der Biobank-Datentreuhänder muss nicht mit einem, sondern mit

zwei Gegenständen (Proben und Daten) umgehen und zwar sowohl bei der Erhebung, bei der Vorhaltung und bei der Herausgabe der Daten und Proben zur Beforschung. Dies folgt aus der Notwendigkeit einer abschnittbezogenen Pseudonymisierung, die unter 4.4 dargestellt und erläutert wird.

Zuletzt sind durch die Einschaltung eines externen Datentreuhänders die Re-Identifizierungsrisiken, die in der Biobank **während** der Vorhaltung bestehen oder sich entwickeln oder die sich aus der Übermittlung von Daten (und Proben) an Externe (Forscher) oder aus dem Rückertrag von Forschungsergebnissen in die Biobank hinein ergeben, nicht beherrschbar. Dies muss innerhalb der Biobank geschehen.

In der Praxis erscheint es damit wenig aussichtsreich, für den Bereich des Biobankengeschäfts einen **externen** Datentreuhänder zu finden, der den oben beschriebenen Anforderungen gereicht wird.

Aus diesem Grund ist eine Modifizierung des klassischen externen Datentreuhändermodells notwendig:
1. Die Funktionen des Datentreuhänders müssen dafür in die Biobank hinein verlagert werden, denn nur dort ist eine Probenhandhabungsinfrastruktur vorhanden.
2. Dem dadurch entstehenden Zusammenfallen von Treuhänder einerseits sowie Daten und Proben nutzender Stelle andererseits muss die Biobank durch die Einführung besonderer Instrumente des Datenschutzes gerecht werden, wie sie sich nach dem Rechtsvergleich als geeignete Maßnahmen und Vorgaben darstellen (insbesondere: durch die Einführung externer Audits). Diese Gedanken werden danach im fünften Abschnitt vorgestellt.

4 Geeignete Mittel des Spenderschutzes

4.1 Spenderschutz durch abschnittbezogene Pseudonymisierung

Wegen der sensiblen Informationen, die Biobanken mit den Spenderproben und -daten verwalten, ist bei ihnen der Einsatz von einem oder mehreren Pseudonymisierungsverfahren notwendig[187]. Die unter dieser Textziffer vorgestellte abschnittbezogene Pseudonymisierung wurde auf dem Workshop „Datenschutzrechtliche Auditierung von Biobanken“ am 4.7.2008 eingeführt[188]. Die folgenden Ausführungen stammen aus einem Beitrag zum Tagungsband zum Workshop „ID-Management und Pseudonymisierung“ der TMF, der am 15.12.2008 in Berlin stattfand[189].

4.1.1 Übersicht

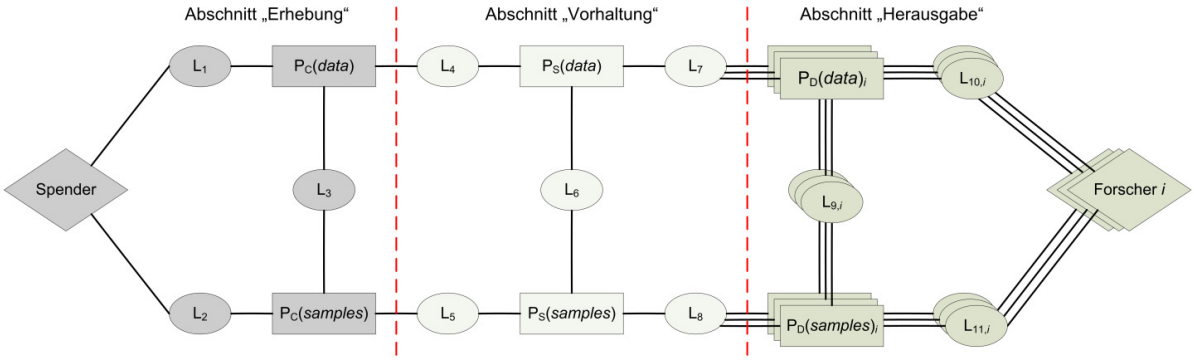

Abb. 1: Darstellung der abschnittbezogenen Pseudonymisierung in den Abschnitten „Erhebung“, „Vorhaltung“ und „Herausgabe“ einer Biobank

Abb. 1 stellt die drei generellen Risikosphären dar, die sich aus den Abschnitten „Erhebung“ („Collection“), „Vorhaltung“ („Storage“) und „Weitergabe“ („Disclosure“) ergeben. Diese Abschnitte sind kennzeichnend für den Datenverarbeitungsgang. Sie kommen in jeder Biobank vor und werden durch bestimmte technische und organisatorische Prozesse realisiert:

- Im Abschnitt „Erhebung“ werden die Daten und Proben des Spenders erhoben und in der Biobank gespeichert. Dieser Abschnitt geht den anderen Abschnitten voraus. Falls Proben desselben Spenders über einen längeren Zeitraum in die Biobank aufgenommen werden, obliegt es den Prozessen in diesem Abschnitt, die Zuordnung zu den schon bisher verfügbaren Proben und Daten (soweit dies gewünscht ist) herzustellen. In diesem Abschnitt besteht der

[187] Vgl. Pommerening, Das Datenschutzkonzept der TMF für Biomaterialbanken; it – Information Technology 49 (2007) 6, 352-359.
[188] Die Vortragsfolien stehen unter https://www.datenschutzzentrum.de/biobank/ zur Verfügung.
[189] Kurzbericht zum TMF-Workshop vom 15.12.2008: http://www.tmf-ev.de/News/tabid/108/articleType/ArticleView/articleId/433/Default.aspx; Beitrag im Tagungsband (im Erscheinen): Hansen/Zimmermann, Anforderungen des Datenschutzes an ID-Management in der medizinischen Forschung.

Kontakt zum Zulieferer der Proben und Daten; dies kann der Spender selbst sein oder beispielsweise eine Arztpraxis, die wiederum im Kontakt mit dem Spender steht.

- Der Abschnitt „Vorhaltung“ hat die Aufgabe, Proben und Daten in ihrer Zuordnung zueinander für einen langen Zeitraum aufzubewahren, aufzubereiten und für definierte Bedarfsfälle verfügbar zu halten.

- Im Abschnitt „Herausgabe“ werden die Daten (oder einander zugeordnete Daten und Proben) an die anfragenden Forschungsteams – unter Berücksichtigung von definierten Bedingungen – gegeben. Dieser Abschnitt unterteilt sich daher in Unterabschnitte, die jeweils einer Herausgabe an ein einzelnes Forschungsteam entsprechen.

Der Weg, den die Proben und Daten nehmen, führt in der Abbildung von links nach rechts. Der Prozess der Rückkopplung von Forschungsergebnissen an die Biobank oder an die Spender wird in der Abbildung nicht als eigener Abschnitt gesehen, sondern würde über den Rückweg, d. h. von rechts nach links, zu realisieren sein.

Die dargestellten Abschnitte bilden unterschiedliche Risikosphären, d. h. aus Sicht der Biobank sind die Risiken für eine ungewollte Herstellung des Personenbezugs oder einen unbefugten Zugriff auf die Proben und Daten unterschiedlich stark beherrschbar: Während im Abschnitt „Vorhaltung“ die Datenverarbeitungsvorgänge rein intern in der Biobank ablaufen, damit unter ihrer Kontrolle stehen und deshalb von ihr rechtlich umfassend verantwortet werden können, ist dies an den Schnittstellen nach außen, nämlich beim Erheben und bei der Weitergabe, nicht der Fall. Aus Sicht der Biobank handelt es sich dort um unsichere Außenbereiche, die von der internen Verarbeitung abzutrennen sind. Dies lässt sich durch eine abschnittbezogene Pseudonymisierung in der Biobank realisieren, die im Folgenden erläutert wird.

4.1.2 Abschnittbezogene Pseudonymisierung

Abschnitt „Erhebung“: Die geeignete Maßnahme des Spenderschutzes besteht in einer ersten Pseudonymisierung. Der an einer AIDS-Studie teilnehmenden Herr A. erhält beispielsweise bei der Erhebung seiner Daten ein Erhebungspseudonym für die Daten ($P_C(data)$ – P steht dabei für „Pseudonym“, C für „Collection“). Liefert Herr A. nicht nur Daten, sondern auch Proben, so müssen die Proben bzw. ihre Zuordnung zu Herrn A. ebenfalls pseudonymisiert werden. Hierbei geht es nicht um ein Entfernen des Personenbezugs aus den vorliegenden Proben (d. h. aus Gewebe oder Körperflüssigkeiten), was im Allgemeinen auch nicht funktionieren würde,[190] sondern nur um die Vergabe der Bezeichner, die für die Probenverwaltung eingesetzt werden.

Hierzu würde deshalb lediglich ein Erhebungspseudonym für die Proben ($P_C(samples)$) vergeben. Da die Handhabung von Daten und Proben auf unterschiedlichen technisch-organisatorischen Wegen erfolgt und dabei unterschiedliche Risiken bestehen, ist es zweckmäßig und anerkannter Stand guter

[190] Siehe z. B. Wellbrock: Datenschutzrechtliche Aspekte des Aufbaus von Biobanken, MedR 2003, 77-82.

Praxis, Daten und Proben je unterschiedliche Pseudonyme zu geben. Dann kann von Datenpseudonymen nicht auf Probenpseudonyme geschlossen werden – und umgekehrt. Dabei muss darauf geachtet werden, dass dennoch die Zuordnung zwischen Daten und Proben zuverlässig erhalten bleibt. Zu den Daten und Proben entstehen in der Folge die Pseudonyme P_C(*data*) und P_C(*samples*) mit den jeweiligen Zuordnungsregeln L_1, L_2 und L_3 (L für „Link“ oder „Linkage rule“), siehe Abb. 1. Das wesentliche Risiko liegt in diesem Abschnitt der Verarbeitung im Bekanntwerden des Zusammenhangs zwischen Name und Erhebungspseudonym. Die Betrachtung des Schadens, der bei einer solchen Kompromittierung der Verkettung zwischen Name und Erhebungspseudonym droht, ergibt, dass dieser weder von der Biobank noch überhaupt sonst reparabel ist; denn dieser Zusammenhang ist ein unveränderliches Geheimnis, das die Biobank zudem nicht allein beherrscht.

Abschnitt „Vorhaltung“: Die zuvor erläuterte, rechtlich begründete Notwendigkeit, beim Wechsel der Risikosphäre (also an „Risikoschwellen“) die Pseudonyme zu tauschen, ergibt, dass die Erhebungspseudonyme am Beginn des folgenden Abschnitts der Vorhaltung für wechselnde Fälle der Beforschung bei der Biobank durch Vorhaltungspseudonyme zu ersetzen sind. Dies führt auf die Vorhaltungspseudonyme P_S(*data*) und P_S(*samples*) sowie auf die drei weiteren Zuordnungsregeln L_4, L_5 und L_6. Das wesentliche Risiko, das nach diesem Pseudonymtausch während der Vorhaltung der Daten und Proben für wechselnde Fälle der Beforschung bei der Biobank besteht, liegt im Bekanntwerden der Verkettung zwischen Erhebungspseudonym P_C(*data*)/P_C(*samples*) einerseits und Vorhaltungspseudonym P_S(*data*)/P_S(*samples*) andererseits. Die Betrachtung des Schadens, der bei Kompromittierung der Verkettung zwischen Erhebungspseudonym und Vorhaltungspseudonym droht, ergibt jedoch im Vergleich zu der hierzu bei den Erhebungspseudonymen dargelegten Sachlage, dass der Schaden hier reparabel ist. Zudem ist es die Biobank, die die Reparatur vornehmen kann – nämlich, indem sie etwa ein neues Vorhaltungspseudonym vergibt und so die kompromittierte Verkettung durch eine neue ersetzt. Das in der Verkettung von Erhebungspseudonym und Vorhaltungspseudonym liegende Geheimnis ist also nicht mehr unersetzlich; zudem kann die Biobank den Austausch gegen ein neues Geheimnis aus eigener Machtvollkommenheit, also ohne Abstimmung mit Dritten, vornehmen.

Abschnitt „Herausgabe“: Gibt die Biobank Daten (und Proben) zur Beforschung heraus, so führt dies dazu, dass der Herrschafts-, Organisations- und Verantwortungsbereich der Biobank verlassen wird. Für Dinge, die außerhalb der Biobank mit den zur Beforschung herausgegebenen Daten (und Proben) geschehen, ist die Biobank nicht verantwortlich. Für eine randscharfe Abgrenzung der Verantwortlichkeit ist es deshalb erforderlich, dass für die Herausgabe zur Beforschung durch externe Forscherteams erneut ein Pseudonymwechsel stattfindet. Dies zeigt Abb. 1 mit den weiteren Pseudonymen P_D(*data*) und P_D(*samples*) sowie den Verkettungen L_7, L_8 und L_9, die jeweils pro Forscherteam vorzusehen sind. Die Verkettungen L_{10} und L_{11} schließlich stellen datentechnisch die Verbindung zu Forscherteams her, die Daten (und Proben) erhalten. Dabei gilt wiederum, was bereits für den Abschnitt der Vorhaltung zu dort gegebenenfalls auftretenden kompromittierten Verkettungen gesagt wurde: Auch im Herausgabe-Abschnitt kann die Biobank notfalls das betroffene Vorhaltungspseudonym ändern und so den eingetretenen Schaden reparieren; dies kann sie ohne Abstimmung mit Dritten tun.

Abschnitt	**Erhebung („Collection“)**	**Risikoschwelle**	**Vorhaltung („Storage“)**	**Risikoschwelle**	**Herausgabe 1 („Disclosure 1“)**	**Herausgabe *i* („Disclosure *i*“)**
Beschreibung	Unsicherer Außenbereich		Sicherer Innenbereich		Unsicherer Außenbereich bei Forscher 1	bei Forscher *i*
Pseudonym-wechsel	Erhebungs-pseudonyme		Vorhaltungs-pseudonyme		Herausgabepseudonyme	
Pseudonym für Daten („*data*“)	$P_C(data)$		$P_S(data)$		$P_D(data)_1$	$P_D(data)_i$
Pseudonym für Proben („*samples*“)	$P_C(samples)$		$P_S(samples)$		$P_D(samples)_1$	$P_D(samples)_i$

Tabelle 1: Pseudonymverwendung pro Abschnitt

Tabelle 1 zeigt im Überblick, welche Pseudonyme in welchem Abschnitt verwendet werden. Dass eine größere Anzahl von Pseudonymen zum Einsatz kommt, ist durch einen nur einmalig anfallenden konzeptionellen Aufwand möglich und kann durch Technik-Einsatz bei wenig laufendem Personalkostenaufwand zuverlässig und kontinuierlich bereitgestellt werden. Der zusätzliche Aufwand gegenüber der Verwendung einer geringeren Anzahl von Pseudonymen ist bedeutungslos, gemessen an dem Nutzen der abschnittbezogenen Pseudonymisierung, bei dem verschiedene Risikosphären wirksam voneinander getrennt und dadurch Verantwortlichkeiten zuverlässig zugeordnet und beherrschbar gemacht werden können. Insbesondere ergibt sich ein Vorteil daraus, dass das unveränderliche Geheimnis der direkten Zuordnung von Proben und Daten zu den Spendern aus der Erhebungsphase nicht im späteren Verlauf durch die interne Datenverarbeitung der Biobank oder die externe Datenverarbeitung bei diversen Forschungsteams korrumpiert werden kann. In diesen späteren Datenverarbeitungsprozessen wird nämlich jeweils mit neuen Pseudonymen gearbeitet.

Eine solche Mehrfach-Pseudonymisierung ist deshalb eine Verfahrensweise, die nicht nur – etwa im Sinne einer „doppelten Naht“, wie dies bei den „double coded samples“ von der Europäischen Medizinagentur[191] nahegelegt wird – zu einem bloß quantitativen Mehr an Sicherheit führt. Der Sicherheitsgewinn ist auch ein qualitativer: Durch ihn werden „unveränderliche Geheimnisse“ gegen „Wegwerfgeheimnisse“ eingetauscht. Der qualitative Unterschied zwischen einerseits einer Verwendung von „unveränderlichen Geheimnissen“, deren Bekanntwerden zu unangenehmen Konsequenzen für die Spender und ihre Privatsphäre führen kann, und andererseits der Verwendung von durch Mehrfach-Pseudonymisierung erzeugten auswechselbaren und organisationseigenen „Wegwerfgeheimnissen“ wird in seinen praktischen Auswirkungen dann deutlich zu Tage treten, wenn ein künftiges Datenschutzrecht Datenverarbeiter dazu verpflichtet, Betroffene von Sicherheitsvorfällen mit Datenschutzverletzungen in Kenntnis zu setzen. Diese Pflicht greift sicher dann, wenn Zuordnungen von Patientennamen zu Erhebungspseudonymen bekannt wurden. Wurden

[191] European Medicines Agency, Understanding the Terminology used in Pharmacogenetics, EMEA/3842/04/Final of 29 July 2004.

dagegen lediglich Zuordnungen zu Pseudonymen kompromittiert, die ihrerseits auf andere Pseudonyme verweisen, was bei abschnittbezogener Mehrfach-Pseudonymisierung eher der Fall sein wird, dann wird man demgegenüber eine solche Informationspflicht im Grundsatz nur annehmen können, wenn die Gefahr besteht, dass durch den fraglichen Sicherheitsvorfall neben der Zuordnungsregel zu einem Folgepseudonym auch die davor liegende erste Zuordnung zu einem Erhebungspseudonym kompromittiert wurde.

Diese Ausführungen haben deutlich gemacht, wie die operativen Erfordernisse von Datentreuhänderschaft **innerhalb** der Biobank realisiert werden können.

Für alle (Daten-) Treuhänder gilt das unter 3.2.2.4.1.1 Ausgeführte: Gegenüber dem Treugeber (Spender) durch Kompetenz überlegene oder in Interessenkonflikten befangene Treuhänder müssen dem Treugeber in proaktiver Weise Transparenz gewähren. Dies gilt in entsprechender Weise dann, wenn – wie hier – die Konfliktbefangenheit daraus entsteht, dass diese Rolle als **interner** Datentreuhänder organisiert ist und sich innerhalb der Biobank befindet, so dass Unabhängigkeit nicht durch organisatorische und institutionelle Vorkehrungen gewährleistet wird. Die allgemein-zivilrechtlich begründete, aus § 666 BGB folgende Pflicht des Treuhänders zu proaktiver Transparenz muss erst recht in einem solchen Fall interner Datentreuhänderschaft gelten, wo bei dem innerhalb der Biobank angesiedelten Treuhänder überlegene Kompetenz und Konfliktbefangenheit gegenüber dem Spender zusammentreffen. Wie diese Transparenz dabei für Biobanken auszugestalten ist, ist im Folgenden unter 4.4 dargelegt.

4.2 Spenderschutz durch Festlegung der Aufbau- und Ablauforganisation

Datenschutz ist grundsätzlich eine Querschnittsaufgabe, die in jedem Bereich eines (Biobank-) Unternehmens umzusetzen ist, da die Datenflüsse gleichermaßen mehrere, wenn nicht alle Bereiche der Biobank betreffen und damit der Datenschutz in der gesamten Organisation an den verschiedensten Stelle zu beachten ist (z. B. bei Eingang, Analyse, und Übermittlung der Daten und Proben). Des Weiteren ist Datenschutz und Datensicherheit eine Daueraufgabe, die einer fortwährenden Überprüfung und Entwicklung bedarf. Um dem Datenschutz gerecht zu werden und Datensicherheit gewährleisten zu können, ist eine fortlaufende Anpassung an den Stand der Technik, die äußeren Umstände sowie die gesetzlichen Rechtsgrundlagen nötig. Um diesen Anforderungen zu genügen, muss der Datenschutz durch eine definierte Aufbau- und Ablauforganisation im Ergebnis durch die Festlegung von Prozessen) unterstützt werden[192]. Dies erfolgt durch die Festlegung von Aufgaben und Abläufen der Vorbereitung, Beratung, Mitwirkung und schließlich der Entscheidung mit dem Ergebnis der Modellierung einer ordnungsgemäßen und damit rechtskonformen und sicheren Datenverarbeitung. Der Datenschutz wird in die Aufbau- und Ablauforganisation der Biobank integriert und damit fester Bestandteil der Unternehmensorganisation, die laufend zu überprüfen und anzupassen ist. Daneben gilt, dass auch die einmal festgelegten datenschutzkonformen Prozesse gesteuert, kontrolliert und angepasst werden müssen, d. h. es muss ein sog. Prozessmanagement bzw. Datenschutzmanagement eingerichtet werden. Bestandteile eines solchen Datenschutzmanagement ist

[192] Bizer, Datenschutz als Gestaltungsaufgabe, DuD 2007, 725, 726.

auch eine revisionssichere und datenschutzkonforme Protokollierung, die konkret überprüfbar ist[193], sowie die Festlegung eines Prozesses für Sicherheitsvorfälle in Abhängigkeit mit ihrer Bedeutung und verbunden mit bestimmten Informationspflichten.[194]

4.3 Spenderschutz durch SOPs

4.3.1 Begriffsbestimmung

Eine Standard Operating Procedure (SOP) ist eine verbindliche (schriftliche) Arbeitsanweisung in einem Unternehmen, welche das Vorgehen innerhalb eines betriebswirtschaftlichen Arbeitsprozesses beschreibt, um die einheitliche Durchführung einer bestimmten Tätigkeit sicherzustellen. Häufig wiederkehrende Arbeitsabläufe werden textlich beschrieben und den Ausführenden erklärend an die Hand gegeben. SOPs führen zu einer Standardisierung von Prozessabläufen. Sie unterliegen einer ständigen Fortentwicklung und Überprüfung, die aufgrund geänderter gesetzlicher Vorgaben oder aufgrund geänderter Organisationsstrukturen notwendig werden. Sie umfassen alle Prozesse, die in einem Unternehmen bestehen, z. B. auch Vertretungsregeln und Weisungsverhältnisse. SOPs stehen damit in indirekten Zusammenhang mit der oben beschriebenen Festlegung der Prozesse, die Voraussetzung für die Erstellung der SOPs.

4.3.2 Vorbild: SOPs bei der Durchführung klinischer Studien

SOPs werden in klinischen Studien verwendet, in denen es darauf ankommt, die Einhaltung immer gleicher Prozessabläufe zu gewährleisten und zu dokumentieren. Die SOPs sind ausdrücklicher Bestandteil der „Guten Klinischen Praxis – Good Clinical Practice“ (international: ICH-GCP). Dies ist ein Standard für Planung, Durchführung, Monitoring, Auditing, Dokumentation, Auswertung und Berichterstattung von klinischen Prüfungen, um sicherzustellen, dass die Daten und die berichteten Ergebnisse glaubwürdig und korrekt sind und dass die Rechte und die Integrität sowie die Vertraulichkeit der Identität der Prüfungsteilnehmer geschützt werden. Die ICH-GCP besteht aus international anerkannten, nach ethischen und wissenschaftlichen Gesichtspunkten aufgestellten Regeln für die Durchführung von klinischen Studien. Dabei stehen der Schutz der Studienteilnehmer und deren informierte Einwilligung sowie die Qualität der Studienergebnisse im Mittelpunkt. Zentrale Dokumente für die Durchführung klinischer Studien wie Prüfplan, Prüferinformation und SOPs sind vorgegeben. Zum Beispiel ist der Sponsor dafür verantwortlich, Qualitätssicherungs- und Qualitätskontrollsysteme mittels schriftlicher SOPs zu implementieren und zu pflegen, um klinische Prüfungen und die Erhebung, Dokumentation sowie das Berichten der Daten in Übereinstimmung mit dem Protokoll, GCP und den geltenden gesetzlichen Anforderungen zu gewährleisten.

In Deutschland regelt die GCP-Verordnung im Detail die Genehmigung und Durchführung klinischer Studien mit Arzneimitteln am Menschen. Sie schreibt die GCP für alle derartigen klinischen Studien verbindlich vor. Im Rahmen einer Reihe von Projekten entwickelt die TMF harmonisierte, standardisierte SOPs für die Durchführung klinischer Prüfungen mit Arzneimitteln und

[193] Bizer, Datenschutz als Gestaltungsaufgabe, DuD 2007, 725, 726.
[194] Bizer, Modernisierung des Datenschutzes: Vier Säulen des Datenschutzes, DuD 2007, 264, 266.

Medizinprodukten für ihre Forschungsverbünde. Das Arbeiten entsprechend der SOPs soll es ermöglichen, den gesetzlichen Verpflichtungen (neues AMG, europäische Direktive 2001/20/EC) und internationalen Anforderungen (ICH-GCP) zu genügen.

4.3.3 Umsetzung in der Biobank-Forschung

SOPs können als selbstregulierende Maßnahme effektiv dazu beitragen, dass der Spenderschutz gewährleistet wird. Die Biobank nimmt für die operative Gestaltung ihrer internen Abläufe zu Einwerbung, Erhebung, Verarbeitung, Analytik, Aufbereitung und Übermittlung an die Forschung, zur Gewährleistung von Spenderrechten sowie zur Qualitätssicherung eine systematische Bestimmung vor und fixiert diese abschließend in betrieblichen Prozessen. Die SOPs werden jährlich auf einen neuen Stand gebracht.

4.4 Spenderschutz durch Codes of Conduct

4.4.1 Verhaltensregeln gem. Art 27 Europäische Datenschutzrichtlinie

Art 27 DSRL verpflichtet die Mitgliedstaaten in allgemeiner Weise, die Ausarbeitung von Verhaltensregeln zu fördern. Unter diesem Begriff sind Vorschriften zu verstehen, die sich eine Berufs- oder Fachorganisation, eine Wirtschaftsbranche oder eine sonstige Organisation selbst gibt, um das Verhalten ihrer Mitglieder oder Angehörigen zu regeln. Eine Verbindlichkeit kommt den Regelungen nicht zu. Begrifflich spricht man auch von Code of Conduct oder – im Bereich der Forschung von Code of Ethics[195]. Im BDSG ist die Bestimmung der DSRL u. a. durch § 38a BDSG umgesetzt worden.

Zur Absicherung der Verarbeitung personenbezogener Daten kommen danach neben den staatlich gesetzten, rechtlichen Vorschriften auch die von den jeweiligen Forschungsdisziplinen formulierten Verhaltensregeln in Betracht (Codes of Conduct[196]). Dabei ist zu beachten, dass diese die gesetzliche Rechtslage nicht verändern, sondern lediglich ergänzen können. Codes of Conduct beschränken sich auf die Feststellung des gesetzlichen Regelungsrahmens und können typische Verarbeitungsbedingung für ihre Disziplin empfehlen. Im Grunde müssen alle Vorgaben des geltenden Datenschutzrechtes berücksichtigt werden. Im Gegensatz zu formellen Gesetzen wird aber auf eine eigenverantwortliche Gestaltung der erforderlichen Prozesse gesetzt. Vorteil ist die höhere Flexibilität der selbstregulierenden Maßnahmen[197]. Allgemeine Datenschutzanforderungen an die Entwicklungszyklen der Datenverarbeitungstechnik und ihre konkreten Anwendungen können im Wege der Selbstregulierung flexibler und zügiger angepasst werden.[198] Diese Selbstregulierung kann dem Staat die Durchsetzung staatlicher Regelungen erleichtern sowie das Vertrauen der Betroffenen in die Integrität der Datenverarbeitung stärken. Sie bieten die Chance, dass sich innerhalb der einzelnen Disziplinen fachspezifisch ein Bewusstsein für Datenschutzprobleme entwickelt, die dann mit Hilfe derartiger Richtlinien reduziert werden könnten[199]. Zuletzt können die Verhaltensregeln einen

[195] Bizer, Forschungsfreiheit und informationelle Selbstbestimmung, S. 237ff.
[196] Bizer, Forschungsfreiheit und informationelle Selbstbestimmung, S. 237ff – er spricht insoweit von einem Code of Ethics.
[197] Allg. zum Datenschutz durch Selbstregulierung: Heil, Datenschutz durch Selbstregulierung, DuD 2001, 129ff.
[198] Bizer, in Simitis (Hrsg.), Bundesdatenschutzgesetz, 6. Auflage 2006, § 38a BDSG, Rn. 9.
[199] Bizer, Forschungsfreiheit und informationelle Selbstbestimmung, S 238.

wichtigen Beitrag zur Transparenz leisten, die Voraussetzung der Verwirklichung der Betroffenenrechte ist.

4.4.2 Vorbild § 161 Aktiengesetz

In Deutschland kann als Vorbild der Corporate-Governance-Kodex herangezogen werden. Die von der Bundesministerin für Justiz im September 2001 eingesetzte Regierungskommission „Deutscher Corporate Governance Kodex“ hat diesen „Code of Conduct“ am 26. Februar 2002 verabschiedet. Der Kodex besitzt über die Entsprechenserklärung gemäß § 161 AktG (eingefügt durch das Transparenz- und Publizitätsgesetz von 2002) eine gesetzliche Grundlage. § 161 Aktiengesetz bestimmt, dass „Vorstand und Aufsichtsrat der börsennotierten Gesellschaft jährlich erklären, dass den vom Bundesministerium der Justiz im amtlichen Teil des elektronischen Bundesanzeigers bekannt gemachten Empfehlungen der ‚Regierungskommission Deutscher Corporate Governance Kodex’ entsprochen wurde und wird, oder welche Empfehlungen nicht angewendet wurden oder werden. Die Erklärung ist den Aktionären dauerhaft zugänglich zu machen.“ Der Corporate-Governance-Kodex stellt wesentliche gesetzliche Vorschriften zur Leitung und Überwachung deutscher börsennotierter Gesellschaften (Unternehmensführung) dar und enthält international und national anerkannte Standards guter und verantwortungsvoller Unternehmensführung. Der Kodex soll das deutsche Corporate Governance System transparent und nachvollziehbar machen. Er will das Vertrauen der internationalen und nationalen Anleger, der Kunden, der Mitarbeiter und der Öffentlichkeit in die Leitung und Überwachung deutscher börsennotierter Gesellschaften fördern. Der Kodex adressiert weiter alle wesentlichen – vor allem internationale – Kritikpunkte an der deutschen Unternehmensverfassung, zum Beispiel die mangelnde Transparenz deutscher Unternehmensführung, die mangelnde Unabhängigkeit deutscher Aufsichtsräte und eingeschränkte Unabhängigkeit der Abschlussprüfer. Die Bestimmungen und Regelungen des Kodex gehen auf jeden einzelnen dieser Kritikpunkte ein und berücksichtigen dabei die gesetzlichen Rahmenbedingungen[200].

4.4.3 Umsetzung in der Biobank-Forschung

Biobanken sind gleichermaßen davon abhängig, dass Lösungen für den Schutz der Privatsphäre und zur Vertrauensbildung bei den Betroffenen getroffen werden. Die Flexibilität der selbstregulierenden Maßnahmen würde der Homogenität der Biobanken Rechnung tragen. Eine Selbstregulierung der Biobanken würde dem Staat die Durchsetzung staatlicher Regelungen erleichtern sowie das Vertrauen der Betroffenen in die Betreiber und die Geheimhaltung ihrer äußerst sensiblen Daten stärken. Daneben können allgemeine Datenschutzanforderungen an die fortschreitenden Entwicklungen der Datenverarbeitungstechnik flexibel und zügig konkretisiert und angepasst werden. Sie bieten daher gerade für Biobanken das erforderliche Bewusstsein für Datenschutzprobleme und können die für die Betroffenen so wesentliche Transparenz schaffen. Es ist jedoch festzuhalten, dass selbstregulierende Elemente keine Alternative zur gesetzlichen Absicherung der Grundkomponenten des Datenschutzes ist.

---

[200] Der Deutsche Corporate-Governance-Kodex ist abrufbar unter: http://www.corporate-governance-code.de/ger/kodex/1.html.

4.5 Spenderschutz durch Transparenz

Transparenz der Datenverarbeitung und der Verantwortlichen ist eine entscheidende Grundbedingung nicht nur für die Einwilligung des Betroffenen. Dieser kann nur tatsächlich freiwillig und informiert in die Verarbeitung seiner Daten einwilligen, wenn er überblicken kann, was tatsächlich mit seinen Daten geschieht und wer sie zu welchem Zweck verarbeitet. Dabei ist es jedoch nicht nur erforderlich, das die Betroffenen sich vor der Einwilligung ausreichend informieren können. Es ist vielmehr notwendig, dass eine laufende Information der Betroffenen stattfindet. Die laufende oder auch sog. nachgeholte Transparenz ist Voraussetzung für die Ausübung und Durchsetzung der Datenschutzrechte der Betroffenen. Beispielsweise ist effektiver Betroffenenschutz über die Möglichkeit des Widerrufs der erteilten Einwilligung überhaupt erst möglich, wenn der Betroffene Kenntnis über die Einwicklung „seiner" Biobank und „seiner" Forschungsprojekte hat. Die folgenden Maßnahmen haben daher sowohl die Information von potentiellen als auch von den aktuellen Spendern im Fokus.

4.5.1 Biobankregister

Die Landschaft der Biobanken ist nicht mehr bzw. kaum noch überschaubar. Dies hat für die Spenderinnen und Spender von Biomaterial, für die Aufsichtsbehörden und für die Öffentlichkeit große Unübersichtlichkeit zur Folge – auch im Hinblick auf die Wahrung der Datenschutzrechte: Es wird für die Betroffenen zunehmend schwerer, in den wechselnden Netzwerken, Verbünden und Ausgründungen die Ansprechpartner für ihre medizinrechtlichen und datenschutzrechtlichen Auskunftsansprüche zu identifizieren. Deshalb liegt es nahe, in Anlehnung an die internationalen und europäischen Empfehlungen bzw. Rechtslagen ein Biobankregister mit obligatorischer Meldepflicht der Forschungsprojekte vorzusehen[201]. Dieses Register könnte z. B. bei der Bundesärztekammer geführt werden. Dabei wäre der Mindest-Meldeinhalt

- Name, Betreiber, gesetzliche Vertretungsverhältnisse und Adresse der Biobank sowie ein spezifisch benannter Ansprechpartner, an den die Spenderin bzw. der Spender sich wegen der Verwendung und Weitergabe der Proben und Daten wenden kann,
- Bezeichnung der Art der Proben und Daten und
- Bezeichnung aller Forschungsprojekte, die mit den Daten und/oder Proben der betreffenden Biobank arbeiten oder in der Vergangenheit gearbeitet haben und des zugeordneten Ansprechpartners.

Forscher in der TMF haben ein Register medizinisch relevanter Biomaterialbanken in Deutschland als Web-basiertes Open-Access-Verzeichnis aufgebaut. Dieses soll in einem Folge-Projekt nach und nach zu einem umfassenden Biobanken-Register ausgebaut werden. Das Register wird dann in deutscher und englischer Sprache zur Verfügung gestellt und nach Inhalt sowie nach Regionen gegliedert.[202]

---

[201] Z. B. entsprechend des Entwurfes des Schweizer Humanforschungsgesetzes, der in Art. 58 eine Meldepflicht für Biobanken vorsieht.
[202] Vgl. http://www.tmf-ev.de/Themen/Projekte/V05801BiobankenRegister.aspx.

4.5.2 Studienregister

Weiter sollte ein Studienregister, das nähere Informationen über die Forschungsprojekte, die mit Daten und Proben arbeiten, eingerichtet werden. Eine ähnliche Einrichtung ist 2005 durch Beschluss der europäischen, amerikanischen und japanischen Pharmaverbände gemeinsam mit dem Internationalen Pharmaverband IFPMA im Bereich der Arzneimittelforschung durch das „Studienregister Verband forschender Arzneimittelhersteller“ geschaffen worden. Ziel dieses Register ist es, jedem zu ermöglichen nachzuvollziehen, welche Ergebnisse bei Arzneimittelstudien mit Patienten herausgekommen sind. Dazu werden die Resultate sämtlicher von forschenden Arzneimittelherstellern gemeinsam mit Kliniken oder Arztpraxen durchgeführten Studien in öffentlich zugängliche Internet-Datenbanken eingestellt. Die lückenlose Publikation aller Studienergebnisse soll dazu beitragen, dass sich Ärzte bei der Behandlung ihrer Patienten und Wissenschaftler bei der Forschungsplanung stets auf den gesamten Wissensstand zu einem Medikament stützen können[203]. Vergleichbares ist auch in der Schweiz im Entwurf des Humanforschungsgesetzes geplant. Die bewilligten Forschungsprojekte sowie eine Zusammenfassung von deren Ergebnissen sollen verpflichtend in einem öffentlich zugänglichen Register aufgenommen werden.[204]

4.5.3 Geschäftsmodellbeschreibung

Der Spender muss nicht nur bei Einwilligung, sondern fortlaufend über die Geschäfte einer Biobank informiert werden. In einer Geschäftsmodellbeschreibung werden die grundsätzlichen Geschäftsziele, -strategien und Praktiken des Unternehmens festgehalten und transparent gemacht. Sie enthält damit für den Spender wichtige Informationen. Folgende Inhalte sollte eine Geschäftsmodellbeschreibung haben:

- Für welche Arten von Forschungsprojekten die Biobank grundsätzlich zur Verfügung stehen will und
- ob grundsätzlich Daten und Proben für wechselnde Projekte der Beforschung erhoben werden sollen.
- Die Biobank beschreibt außerdem die Zielgruppe der Personen, die als Spender oder gegebenenfalls als Kontrollgruppe für die Zulieferung von Daten oder von Proben und Daten infrage kommen. Dabei erläutert sie, ob auch Kinder, Behinderte oder altersdemente Personen als Spender infrage kommen, falls ja, gibt sie allgemein an, welche besonderen betrieblichen Schutzmechanismen sie hierfür einhalten will, ob die Daten auch aus dem Behandlungszusammenhang erhoben werden.
- Die Biobank gibt die Zwecke der Forschung an, denen sie in der Zukunft dienen möchte.
- Die Biobank beschreibt die Einheiten ihrer Aufbauorganisation und die gewählte Rechtsform.

4.5.4 Biobank-Policy

Policys sind Leitlinien, in denen sich ein Unternehmen auf die Einhaltung bestimmter Grundsätze verpflichtet und dies nach außen bekannt gibt. Nicht entscheidend ist, ob diesen Grundsätzen eine

---

[203] Vgl. Homepage des Verbandes Forschender Arzneimittelhersteller e.V., http://www.vfa.de/de/index.html.
[204] Art. 72 Abs. 1 HFG-Entwurf.

gesetzliche Pflicht zugrunde liegt[205]. Die Leitlinien haben oftmals sowohl eine Verpflichtung der Einhaltung der gesetzlichen Vorschriften, als auch eine Selbstverpflichtung zum Inhalt, ohne dass eine entsprechende gesetzliche Verpflichtung besteht.

4.5.5 Publizität von Spenderaufklärung und Spendereinwilligung als Textmuster

Um die erforderliche Informiertheit des Betroffenen vor seiner Einwilligung herzustellen, veröffentlicht die Biobank die von ihr gegenüber den Spendern verwendeten Spenderaufklärungen und Spendereinwilligungen an leicht zugänglicher Stelle im Internet. Dies gibt den Betroffenen ausreichend Gelegenheit, eine Entscheidung über die Verarbeitung ihrer Daten zu treffen. Die Spendereinwilligung sollte verständlich gestaltet und mehrsprachig vorhanden sein.

4.5.6 Jährlicher Datenschutzbericht der Biobank

Nicht nur im Zeitpunkt der Einwilligung, sondern fortlaufend ist eine Information der Betroffenen notwendig. Da die Weiterverwendung der Daten in der Biobank im Regelfall für einen längeren Zeitraum geplant ist, müssen die Betroffenen über die Entwicklung der Biobank, deren Forschungsprojekte, deren Datenschutzpolicy informiert werden. Andernfalls laufen ihre Rechte, insbesondere ihre Rechte auf Auskunft, Widerruf und Löschung ins Leere. Biobanken sollten daher einen jährlichen Datenschutzbericht veröffentlichen, den sie im Internet zeitnah an leicht auffindbarer Stelle einstellen. In dem Bericht informiert die Biobank über:

- ihre eigene Entwicklung, d. h. ihre eingeworbenen Spenden und Gegenstände der Forschungsprojekte, die Entwicklung bei Sponsoren und der verwendeten Analysemethoden in allgemein verständlicher Form;
- ihre Forschungsprojekte, insbesondere welche abgeschlossen sind und welche nicht, ob eine Spenderkontakt erfolgen soll, wer der Auftraggeber und der Sponsor ist, was Gegenstand, Zweck und Ziel des Projektes, die Verantwortlichen und Ansprechpartner;
- die Forschungsergebnisse in der Vergangenheit aus eigener und fremder Forschung sowie die Aufnahme der gewonnenen Daten in der Biobank;
- das Verfahren bei der Umsetzung von Spenderrechten sowie über die Umsetzung von Spenderrechten in der Vergangenheit, über antragsgemäße oder verweigerte Auskünfte an Spender sowie über vollzogene oder verweigerte Teilnahmewiderrufe;
- illegale und legale Zugriffe auf ihre Datenbestände;
- die Ethikvoten, die ihre Forschungsprojekte betreffen (durch Veröffentlichung oder der Angabe einer Quelle; wurde auf ein Ethikvotum verzichtet, gibt sie die Gründe dafür an);
- den oder die Datenschutzbeauftragte(n).

4.6 Spenderschutz durch Auditierung

Eine Auditierung führt vor allen Dingen zur Transparenz der Unternehmensprozesse und zur Erhöhung der Rechtssicherheit in Bezug auf die Umsetzung der rechtlichen Verpflichtungen. Durch die Bescheinigung der Gesetzeskonformität wird das Vertrauen der Verbraucher gestärkt und dem Unternehmen eine verbesserte Stellung am Markt verschafft. Audits sind daher von ihrer Zielsetzung

[205] Vgl. z. B. das Leitbild und die Leitlinien der Charite: http://www.charite.de/charite/organisation/leitbild/; http://www.charite.de/charite/organisation/leitbild/umweltleitlinien/.

eine geeignet Maßnahme, den Spenderschutz in Biobanken zu verbessern und das Vertrauen der Betroffen zu erhöhen. Die Auditierung von Biobanken ist Gegenstand des folgenden Kapitels.

5 Auditierung von Biobanken

5.1 Qualitätssicherung durch ungeregelte und (staatlich) geregelte Konformitätsbewertung

5.1.1 Konformitätsbewertungen im Allgemeinen

Bei einer Konformitätsbewertung handelt es sich um die Darlegung, dass festgelegte Anforderungen erfüllt sind. Damit ist die Überprüfung von Produkten, Dienstleistungen, Prozessen, Systemen und Personen durch Inspektions- oder Zertifizierungsstellen gemeint sowie die Überprüfung dieser Stellen durch eine übergeordnete unabhängige Einrichtung[206]. Die Konformitätsbewertung ist das Bindeglied zwischen Qualitätsvorgaben für Produkte und Dienstleistungen und dem Anspruch der Verbraucher nach Waren, die diesen Vorgaben entsprechen[207]. Dabei kann man zwischen dem geregelten und dem ungeregelten Bereich unterscheiden, wobei eine strikte Trennung zwischen diesen Bereichen ausschließlich in Deutschland üblich ist. In den anderen europäischen Ländern ist dies weniger gebräuchlich und es hat sich zumeist eine zentrale Akkreditierungsstelle herausgebildet[208]. Als gesetzlich geregelt gelten diejenigen Bereiche, in denen durch Rechtsvorschriften Regelungen bezüglich der Akkreditierung, Zertifizierung, Prüfung und ähnlicher Verfahren festgelegt sind. Dabei kann es sich sowohl um nationale als auch um europäische Rechtsvorschriften handeln. Deren Einhaltung muss eine Konformitätsbewertungsstelle feststellen, deren Anerkennung durch eine öffentliche Stelle erfolgt, die aufgrund landesrechtlicher Vorschriften dazu ermächtigt ist. Solche Regeln existieren insbesondere als Zulassungs- und Ausübungsregelungen, die den garantierten Marktzutritt beschränken bzw. die Ausübung erleichtern. Unerheblich für die Einordnung in den geregelten Bereich ist, ob die Teilnahme an dem Konformitätsbewertungsverfahren verbindlich oder verpflichtend ist[209]. Gehen die Rechtsvorschriften, die die Konformitätsbewertung regeln, auf europäisches Sekundärrecht zurück (insb. als Umsetzung einer EU-Richtlinie ins deutsche Recht), handelt es sich um den harmonisierten geregelten Bereich, weil hier die Anwendung der Konformitätsbewertungsverfahren aufgrund harmonisierten europäischen Rechts erfolgt[210]. In diesem sog. geregelten Bereich soll die Zertifizierung sicherstellen, dass die grundlegenden Anforderungen der jeweiligen europäischen Richtlinien bzw. des nationalen Rechts beachten wurden.[211]

Als gesetzlich nicht geregelter Bereich werden die Bereiche bezeichnet, in denen weder auf nationaler noch auf europäischer Ebene Rechtsvorschriften bezüglich der Akkreditierung, Zertifizierung und Prüfung existieren. Dennoch werden in diesen Bereichen Akkreditierungen durchgeführt, da der Markt dies erfordert. Die Prüfungen basieren auf freiwilligen Verträgen und dienen der Vertrauensbildung im Geschäftsverkehr[212].

---

[206] Ernsthaler, Strübbe, Bock, Zertifizierung und Akkreditierung technischer Produkte, S. 27.
[207] Ernsthaler, Strübbe, Bock, Zertifizierung und Akkreditierung technischer Produkte, S. 39.
[208] Ernsthaler, Strübbe, Bock, Zertifizierung und Akkreditierung technischer Produkte, S. 86f.
[209] Sog. geregelten Bereich im engeren Sinn: Kennzeichnend ist ausschließlich, dass die Konformitätsbewertung durch Rechtsvorschriften vorgesehen bzw. vorgeschrieben ist. Zum Teil wird ein engerer Begriff verwendet, der nur den Bereich umfasst, in dem die Konformitätsbewertung durch Rechtsvorschriften vorgesehen bzw. vorgeschrieben und die Teilnahme verbindlich ist, vgl. Röhl, Konformitätsbewertung in Deutschland, S. 28.
[210] Röhl, Konformitätsbewertung in Deutschland, S. 29.
[211] Vgl. Ernsthaler, Strübbe, Bock, Zertifizierung und Akkreditierung technischer Produkte, S. 29.
[212] Ernsthaler, Strübbe, Bock, Zertifizierung und Akkreditierung technischer Produkte, S. 91.

5.1.2 Konformitätsbewertung im ungeregelten Bereich

Produktbewertungen wurden ursprünglich ausschließlich von privater Seite vergeben. Dabei wurde früh von staatlicher Seite Einfluss darauf genommen wurde, dass sich Gütevereinigungen bilden, die solche Siegel auf der Grundlage von Prüfungen vergeben und dass die Einhaltung der Evaluierungs-, Prüfungs- und Siegelungs-Regeln auch kontrolliert wird[213]. Kennzeichnend für Evaluation und Konformitätsprüfung im ungeregelten Bereich ist Folgendes:

1. Der zu prüfende Produktanbieter gibt sich seine materiellen Qualitätsregeln selbst. Soweit im rechtsgeschäftlichen Verkehr zu einer bestimmten Frage zwingendes Recht besteht oder sich Regeln guter Praxis etabliert haben, ist der Produktanbieter jedoch nicht mehr frei, hiervon abzuweichen[214].
2. Für das Verfahren der Umsetzung betrieblicher Qualitätsregeln und ihrer Nachprüfung wird regelmäßig auf internationale technische Normenstandards Bezug genommen. Üblicherweise sind dies die ISO-Standards der Normenreihen 17000 ff. (allgemeine Konformitätsprüfung) und 27000 ff. (Sicherheitsmanagementsysteme). Das Abweichen von derartigen Standards dürfte im Zuge der allgemeinen Globalisierung der Wirtschaftsbeziehungen zumindest mittelfristig die begründungsbedürftige Ausnahme werden.
3. Die Qualität der prüfenden Stelle wird üblicherweise durch Akkreditierung bzw. einer staatlichen Akkreditierungsreferenz sichergestellt. In Deutschland sind die Zertifizierungsorganisationen üblicherweise akkreditiert und stehen untereinander im Wettbewerb. Akkreditierung und Zertifizierung unterbleiben deshalb im Grundsatz dort, wo dafür kein Markt vorhanden ist – der Staat tritt durch die Bundesanstalt für Materialforschung und -prüfung (BAM) lediglich moderierend auf. In anderen EU-Staaten wird dagegen die Sicherstellung eines Zertifizierungswesens durch das Angebot einer einheitlichen staatlichen Akkreditierungsreferenz für den geregelten und den ungeregelten Bereich als Staatsaufgabe angesehen[215].

5.1.3 Konformitätsbewertung im geregelten Bereich

Als sich Ende der 1980er Jahre – maßgeblich angetrieben durch die Europäisierung des Rechts – das Verständnis von den Aufgaben des Staates zu wandeln beginnt, nimmt die Bedeutung von Auditierung und Zertifizierung deutlich zu. Dieser Prozess wird schlagwortartig als „Wandel vom Eingriffs- und Erfüllungsstaat zum Gewährleistungsstaat“ bezeichnet. Der Staat gibt danach nicht nur Aufgaben gänzlich auf (Aufgabenprivatisierung), sondern er behält in einem weiteren Bereich zwar seine Aufgaben, lässt sie aber durch Private ausführen (Verfahrensprivatisierung). Maßgeblicher Grund für die Verfahrensprivatisierung ist dabei die Beschleunigung des technischen Wandels auf allen technikrechtlichen Feldern, für dessen zeitnahe und kontinuierliche Überwachung den zuständigen

---

[213] Hierzu sei etwa für Deutschland auf den historischen Reichsausschuss für Lieferbedingungen (RAL) hingewiesen, der im heutigen RAL-Verein fortlebt Näheres unter http://www.ral.de/.
[214] Die Entwicklung solcher Regeln guter Praxis kann auch durch internationale Rechtsentwicklungen befördert werden, wie sie etwa vom US-amerikanischen Sarbanes-Oxley-Act ausgehen. Das Gesetz wurde nach den Bilanzskandalen des Jahres 2002 eingeführt. Es führte die Verpflichtung zur Führung besonderer Audit- und Kontrollsysteme zur Unterstützung der korrekten Rechnungslegung im Unternehmen ein. Es gilt auch für ausländische Unternehmen, die an US-Börsen notiert sind.
[215] Vgl. dazu die Darstellungen zu den einzelnen Ländern weiter unter 5.2 ff.

Stellen die Kompetenzen und das Personal fehlen. Dieser Wechsel in den Erfüllungszuständigkeiten wird organisatorisch durch Akkreditierung, Zertifizierung und ggf. Siegelvergabe realisiert.

Ergebnis sind Sachbereiche, in denen die Regelungserfüllung Staatsaufgabe bleibt, der Regelungsvollzug dagegen auf Private verlagert ist, und wo der Zertifizierte seine Regelkonformität durch den Hinweis auf seine Zertifizierung und ggf. durch die Verwendung eines diesbezüglichen staatlich regulierten Gütesiegels nachweisen kann. Die Zertifizierung wird dabei von einer unabhängigen Stelle vorgenommen, die wegen ihrer eigenen Prüfungsqualifikation gewöhnlich einer besonderen Anerkennung bedarf. Verkürzend spricht man von der „regulierten Selbstregulierung“ im geregelten Bereich.

Gesetzlich geregelte Zertifizierungen können freiwillig oder verpflichtend sein. Freiwillige Zertifizierungen sind für den erfolgreich Zertifizierten vielfach mit der Möglichkeit verbunden, ein Gütesiegel zu führen. Das Gütesiegel kann vom Zertifizierten gegenüber Dritten (dem Markt, den Verbrauchern) als Qualitätsnachweis zur Stärkung der eigenen Wettbewerbsposition eingesetzt werden. Es geht im geregelten Bereich außerdem mit verminderten Pflichten zur Duldung staatlicher Kontrollen einher oder erzeugt gegenüber staatlichen Stellen (Behörden) eine grundsätzlich bindende Qualitätsvermutung. Manche gewerbliche Tätigkeiten dürfen überhaupt nur nach entsprechender zwingender Zertifizierung (und ggf. Gütesiegelung) ausgeübt werden. Die Mehrheit der Gegenstände des geregelten Bereichs rechnet man dem europarechtlich vereinheitlichten, sogenannten „harmonisierten“ geregelten Bereich zu. Auf europarechtlicher Ebene (für den traditionellen harmonisierten Bereich, in dem zertifizierende Stellen der EG-Kommission zu notifizieren sind) steht derzeit auf der Agenda, dafür zu sorgen, dass der Kommission nur noch Stellen notifiziert werden, die auch akkreditiert sind[216].

Neben der Herstellung von Markttransparenz dienen Auditierung und Zertifizierung auch Zwecken der Gefahrenabwehr und des Verbraucherschutzes. Auditierungen, Zertifizierungen und ggf. Gütesiegelungen zu Zwecken des Datenschutzes kennt der geregelte bzw. der europarechtlich harmonisierte geregelte Bereich bisher kaum[217].

5.1.4 Zertifizierungsverfahren

Es wird zwischen einstufigen und zweistufigen Zertifizierungsverfahren unterschieden. Bei einem einstufigen Zertifizierungsverfahren wird die Prüfung und Bewertung von einer Stelle vorgenommen, die zugleich bei positivem Ergebnis die Zertifizierung vornimmt. Das Bremer Datenschutzgütesiegel wird zum Beispiel nach einem einstufigen Zertifizierungsverfahren vergeben[218]. Bei einer zweistufigen Zertifizierung überprüft eine von den Prüfenden unabhängige Zertifizierungsstelle in einem zweiten, die Qualität der Zertifizierung sichernden Schritt, ob das Gutachten des Prüfenden vollständig, schlüssig und nachvollziehbar ist und verleiht das Zertifikat. Dem Schleswig-

[216] Arbeitsdokument der EG-Kommission zur Reform der Vorschriften über die Akkreditierung im harmonisierten Bereich vom 14.2.2007, vgl. unter http://ec.europa.eu/enterprise/regulation/internal_market_package/docs/executive_summary_sec_2007_0174_de.pdf .
[217] Weitere Ausführungen dazu unter 5.2 ff.
[218] Weitere Ausführungen dazu unter 5.2.1.4.2.

Holsteinischen Gütesiegel sowie dem europäische Gütesiegel EuroPriSe liegen zum Beispiel zweistufige Zertifizierungsverfahren zu Grunde[219].

5.2 Konformitätsbewertung in ausgewählten europäischen Ländern anhand von Beispielen

5.2.1 Deutschland

5.2.1.1 Organisation des Akkreditierungswesens

Akkreditierung, Auditierung und Zertifizierung sowie ggf. Gütesiegelung sind für Deutschland uneinheitlich geregelt. Ein übergreifendes Akkreditierungsgesetz fehlt, steht aber seit Jahren auf der politischen Agenda[220]. Eine explizite Konformitätspolitik zu Gegenständen des ungeregelten Bereichs gibt es nicht. Die akkreditierenden Organisationen des geregelten und des ungeregelten Bereichs sind im Deutschen Akkreditierungsrat (DAR) zusammengeschlossen[221]. Die Geschäftsstelle dieses Gremiums besteht bei der BAM, die eine bundesunmittelbare, nicht rechtsfähige Anstalt des öffentlichen Rechts im Geschäftsbereich des Bundesministeriums für Wirtschaft ist[222]. Die Akkreditierungsorganisationen des nichtgeregelten Bereichs sind in Deutschland die privatwirtschaftlichen Organisationen DACH[223], DAP[224], DATech[225], GA-A[226], GAZ[227] und TGA[228]. Die genannten Organisationen stehen untereinander in weiten Bereichen in Wettbewerb. Diejenigen Stellen, deren Akkreditierungen den gesetzlich geregelten Bereich betreffen, sind innerhalb des Deutschen Akkreditierungsrats in der Koordinierungsgruppe des gesetzlich geregelten Bereichs (KOGB) organisiert. Geschäftsstellenfunktion für die KOGB übt die Bundesnetzagentur aus[229]. Eine Vielzahl der gesetzlich geregelten Bereiche geht inzwischen auf Regulierungen der EG zurück[230].

Im Datenschutzbereich hatte der Bundesgesetzgeber 2001 zur Stärkung des Datenschutzes § 9a in die Vorschriften des BDSG eingefügt. Dieser bestimmt: „Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und Daten verarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt“. Im September 2007

---

[219] Weitere Ausführungen dazu unter 5.2.1.4.1 und 5.2.7.
[220] Vgl. Pressemitteilung des Bundeswirtschaftsministeriums (BMWi) vom 6.5.2004 „Wirtschaft begrüßt Clements Vorschläge zur Neuordnung der Akkreditierung“ unter http://www.bmwi.de/Navigation/wirtschaft,did=32012.html, Mitteilungen über einen Workshop im BMWi vom 27.7.2006 unter http://www.bmwi.de/BMWi/Navigation/Service/Veranstaltungen/dokumentationen,did= 148670.html.
[221] Vgl. http://www.dar.bam.de/.
[222] Vgl. http://www.bam.de/de/ueber_uns/rechtsgrundlagen/index.htm.
[223] Deutsche Akkreditierungsstelle Chemie GmbH, Frankfurt/Main, http://www.dach-gmbh.de/.
[224] Deutsches Akkreditierungssystem Prüfwesen GmbH, Berlin-Adlershof, http://www.dap.de/.
[225] Deutsche Akkreditierungsstelle Technik GmbH, Frankfurt/Main, http://www.datech.de/.
[226] GA-A – German Accreditation Association e.V., Bonn-Bad Godesberg, http://www.ga-a.de/.
[227] Gesellschaft für Akkreditierung und Zertifizierung mbH, Düsseldorf, http://www.gaz-online.de/?menue=0.
[228] Trägergemeinschaft für Akkreditierung GmbH, Frankfurt/Main, http://www.tga-gmbh.de/.
[229] http://www.bundesnetzagentur.de/enid/3d2b4ebdafbb248c90a3e81533258a0b,0/Anerkennung_Kon formitaets-Bewertungsstellen/Geschaeftsstelle_fuer_die_Koordinierung_von_Stellen_im_g_hg.html.
[230] Vgl. unter http://ec.europa.eu/enterprise/newapproach/standardization/harmstds/reflist.html.

hatte die Bundesregierung einen Entwurf für ein Bundesdatenschutzaudit-Gesetz veröffentlicht[231]. In dem Entwurf[232] war ein einstufiges Zertifizierungsverfahren vorgesehen sowie eine Auditierung durch private Stellen (sog. Kontrollstellen)[233]. Der Entwurf wurde während der 16. Wahlperiode des Deutschen Bundestags nicht beschlossen.

5.2.1.2 Beispiele aus dem geregelten Bereich

5.2.1.2.1 Medizinprodukterecht

Wer in Deutschland Medizinprodukte in Verkehr bringen will, benötigt dazu gemäß § 6 Absatz 2 des Medizinproduktegesetzes (MPG) für jedes Produkt eine vorherige erfolgreiche Produktzertifizierung. Das MPG ist die deutsche Umsetzung der Richtlinie 93/42/EG. Die Einrichtung des Verfahrens der Akkreditierung ist auf der Grundlage von § 15 MPG erfolgt; akkreditierende Stelle ist die Zentralstelle der Länder für Gesundheitsschutz bei Arzneimitteln und Medizinprodukten (ZLG) in Bonn[234]. Akkreditierte Stellen sind zugelassene Prüflabore, ihre Akkreditierung richtet sich nach §§ 15 Absatz 1 i. V. m. Absatz 4 MPG sowie § 37 MPG. Das Verfahren der Prüfung und Auditierung/Zertifizierung eines Medizinprodukts durch ein akkreditiertes Prüflabor richtet sich nach den Regeln über die Vergabe von CE-Kennzeichen[235]. Dieses wird gemäß § 6 Absatz 2 MPG erteilt, wenn die Anforderungen von § 7 MPG erfüllt sind und die Konformitätsbewertung gem. § 37 MPG erfolgreich war.

5.2.1.2.2 Umweltaudit[236]

Unternehmen und Körperschaften des öffentlichen Rechts können ihr Umweltmanagement nach dem „Gemeinschaftssystem für Umweltmanagement und Umweltbetriebsprüfung – Eco Management and Audit Scheme – EMAS“ zertifizieren lassen. Rechtsgrundlagen sind die EG-Verordnung 761/2001 (EMAS-VO) und ihre deutsche Umsetzung im Umweltauditgesetz (UAG) sowie die in diesem Zusammenhang erlassenen Rechtsverordnungen. Die Einrichtung des Verfahrens der Akkreditierung ist auf der Grundlage von § 28 UAG erfolgt; akkreditierende Stelle ist die Deutsche Akkreditierungsgesellschaft für Umweltgutachter GmbH (DAU) in Bonn[237]. Akkreditierte Stellen sind zugelassene Umweltgutachter; ihre Akkreditierung richtet sich nach § 4 ff. UAG i. V. m. der UAG-Zulassungsverfahrensverordnung (UAGZVV)[238]. Die eine Zertifizierung anstrebende Organisation muss bei sich ein Umweltkonzept implementiert haben, das die betrieblichen umweltbezogenen Organisationsziele und Verfahrensweisen ausweist. Dies schließt eine Umweltprüfung der

---

[231] Entwurf eines Bundesdatenschutzauditgesetzes (BDsAuditG), abrufbar unter: http://www.datenschutzzentrum.de/bdsauditg/20070907-entwurf-bdsauditg.pdf.
[232] Gesetzentwurf der Bundesregierung zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften, abrufbar unter http://dip21.bundestag.de/dip21/btd/16/120/1612011.pdf.
[233] §§ 3ff des Entwurfs.
[234] Vgl. http://www.zlg.de/.
[235] § 6 Absatz 1 MPG. Das CE-Kennzeichen wurde durch die Richtlinie 93/68/EWG eingeführt. In Deutschland ist es in § 6 des Gesetzes über technische Arbeitsmittel und Verbraucherprodukte (GPSG) und in den Rechtsverordnungen gem. § 3 GPSG geregelt.
[236] Auch sog. Öko-Audit. Dieses zählt zum geregelten Bereich, wenn man diesen weit auslegt, weil die Kriterien und die Anforderungen gesetzlich geregelt sind, vgl. Röhl, Konformitätsbewertung in Deutschland, S. 28.
[237] §§ 28 UAG i. V. m. § 1 UAG-Beleihungsverordnung; zur DAU vgl. http://www.dau-bonn-gmbh.de.
[238] § 21 Abs. 1 Nr. 1 UAG, vgl. http://www.uga.de/?warp=pup, insbes. die UAG-Fachkunderichtlinie, die UAG-Aufsichtsrichtlinie, die UAG-Prüferrichtlinie sowie die UAG-Zertifizierungsverfahrensrichtlinie die die Umweltgutachter bei der Zertifizierung auf die Norm ISO 14001 festlegt.

betrieblichen Tätigkeiten, Produkte und Dienstleistungen ein. Es muss ein besonderes Umweltmanagementsystem eingerichtet sein, regelmäßig eine interne Umweltbetriebsprüfung stattfinden und als Abschluss eine „Umwelterklärung“ abgegeben werden. Das Verfahren der Prüfung und Auditierung / Zertifizierung eines Umweltmanagementsystems durch einen akkreditierten Umweltgutachter richtet sich nach den Regeln, die in den Anhängen I bis VII der EMAS-VO festgelegt sind. Die Zertifizierung endet mit der Gültigerklärung der Umwelterklärung der zertifizierten Organisation durch den Umweltgutachter; die Erteilung von Gültigerklärungen ohne die Voraussetzungen dieser Vorschriften ist gem. § 19 UAG verboten und wird mit einer Ordnungswidrigkeit geahndet.[239] Nach erfolgreicher Zertifizierung wird die zertifizierte Organisation in ein öffentliches Register aufgenommen, das online abgefragt werden kann[240]. Die Zertifizierung berechtigt zur Führung des EMAS-Siegels. Dies soll für die zertifizierte Organisation zu Kostenvorteilen und zu einem Wettbewerbsvorteil im Markt führen. Zudem gelten für das zertifizierte Unternehmen die rechtlichen Vorteile der EMAS-Privilegierungsverordnung (EMASPV), d. h. insbesondere Erleichterungen bei Anzeige- und Mitteilungspflichten, Verzicht auf die Bestellung eines Betriebsbeauftragten in einigen Fällen, Entfallen von Berichtspflichten und Verfahrenserleichterungen bei der Ermittlung von Emissionen[241].

5.2.1.2.3 Geprüfte Sicherheit – GS-Zeichen[242]

Unternehmen, die technisches Gerät zur Nutzung am Arbeitsplatz oder für Verbraucher in Verkehr bringen, können ihre Produkte freiwillig mit dem GS-Zeichen versehen lassen. Rechtsgrundlage ist § 7 des Gesetzes über technische Arbeitsmittel und Verbraucherprodukte (GPSG). Die Prüfung ist zweistufig, die erste Stufe bildet eine Baumusterprüfung, die zweite eine Prüfung, ob die Produktion die technischen Spezifikationen des Baumusters einhält[243]. Dies schließt die Duldung von Kontrollen der laufenden Produktion ein.[244] Die Länder haben durch Staatsvertrag die Zentralstelle der Länder für Sicherheitstechnik in München als akkreditierende Stelle eingerichtet[245]. Akkreditierte Stellen sind zugelassene Ingenieurbüros, Prüflabore und vergleichbare Firmen, ihre Akkreditierung richtet sich nach § 11 Absatz 1 GPSG. Gemäß § 11 Absatz 4 GPSG führt die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin ein Register der akkreditierten Stellen, das Register ist online abrufbar[246]. Die Stellen stehen untereinander im Wettbewerb, der Unternehmer hat die freie Wahl, bei welcher zugelassenen Stelle er für sein Produkt die GS-Zeichen-Prüfung vornehmen lässt. Das Verfahren der Prüfung und Auditierung / Zertifizierung eines Produktes für die Vergabe eines GS-Zeichens durch die akkreditierte Stelle richtet sich nach § 7 Abs. 1 Satz 2 Nr. 1 und 2 GPSG. Das vergebene GS-Kennzeichen soll dem Unternehmer für sein Produkt am Markt gegenüber Verbrauchern und

---

[239] § 37 Nr. 9 UAG.
[240] § 32 UAG; das Register ist abrufbar unter http://www.emas-register.de/.
[241] §§ 2, 3 und 4 EMASPV, weitere Erleichterungen in §§ 5-8 EMASPV.
[242] Dieses Konformitätsbewertungsverfahren zählt zum geregelten Bereich, wenn man diesen weit auslegt, weil die Kriterien und die Anforderungen gesetzlich geregelt sind, vgl. Röhl, Konformitätsbewertung in Deutschland, S. 28.
[243] § 7 Abs. 1 Satz 2 Nr. 1 und 2 GPSG.
[244] § 7 Abs. 2 Satz 1 GPSG.
[245] Abkommen über die Zentralstelle für Sicherheitstechnik vom 16. und 17.12.1993, geändert durch Abk. vom 16.12.2003, zugänglich unter http://www.zls-muenchen.de/de/doku_pdf/abkommen-zls.pdf.
[246] § 11 Abs. 4 GPSG, abrufbar unter: http://www.baua.de/de/Geraete-und-Produktsicherheit/Pruefstellenverzeichnisse/Kontrolle-GS-Zertifikate/Suche_20nach_20GS-Pr_C3_BCfstellen/GS-Pr_C3_BCfstellen.html__nnn=true.

Unternehmen Wettbewerbsvorteile verschaffen; diese Wirkung haben im gewerblichen Bereich insbesondere die berufsgenossenschaftlichen Unfallverhütungsvorschriften[247], die Arbeitgeber veranlassen, bei der Auswahl der Arbeitsmittel für ihre Arbeitnehmer Geräte mit GS-Zeichen zu bevorzugen.

5.2.1.2.4 Akkreditierung nach der Fahrerlaubnisverordnung

Wer die Fahreignung anderer begutachten oder technische KFZ-Prüfungen vornehmen will oder wer Personen, die ihre Fahrerlaubnis verloren haben, Kurse zur Wiedererlangung der Fahreignung anbieten möchte, benötigt dafür eine Akkreditierung bei der Bundesanstalt für Straßenwesen, § 72 Absatz 2 der Fahrerlaubnisverordnung (FeV). Die Bundesanstalt für Straßenwesen verfährt bei der Vergabe der Akkreditierung nach DIN EN 45010[248]. Akkreditierte Stellen sind die amtlich anerkannten Stellen und Prüfer bzw. die gesetzlich zuständigen Stellen nach den §§ 66, 69 und 70 FeV. Diese Stellen müssen im Hinblick auf die von ihnen angebotenen Dienstleistungen der Norm DIN EN 45013 entsprechen[249].

5.2.1.3 Beispiele aus dem ungeregelten Bereich

Es gibt in Deutschland im privaten Bereich zahlreiche (zumeist markenbasierte) Gütesiegel, die nach entsprechender Evaluation und Konformitätsprüfung vergeben werden. Beispielhaft seien hier aus dem Bereich der Lebensmittel aus naturnaher Landwirtschaft etwa die Siegel Bioland[250], Biopark, Demeter und Ecovin genannt. Die materiellen Anforderungen der betreffenden Evaluierungs- und Prüfschemata sind dabei üblicherweise selbstgesetztes Qualitätsrecht der Wirtschaft, zumeist eines Markenverbandes.

5.2.1.4 Beispiele aus dem Datenschutzbereich

5.2.1.4.1 Datenschutz-Gütesiegel Schleswig-Holstein

Unternehmen können IT-Produkte, die zur Nutzung durch öffentliche Stellen in Schleswig-Holstein geeignet sind, auf ihre Datenschutzkonformität hin überprüfen und zertifizieren lassen[251]. Mit dem Datenschutz-Gütesiegel wird die Vereinbarkeit des Produktes mit den Vorschriften über den Datenschutz und die Datensicherheit festgestellt[252]. Die materiellen Anforderungen an die Produkte und das Verfahren sind in der Datenschutzauditverordnung (DSAVO – auch sog. Gütesiegelverordnung) geregelt.[253] Das ULD hat zur Konkretisierung einen Anforderungskatalog herausgegeben. Dieser ist in vier verschiedene Komplexe unterteilt und benennt exemplarisch Datenschutz- und Datensicherheitsanforderungen, die in erster Linie aus dem Landesdatenschutzgesetz (LDSG-SH) und der schleswig-holsteinischen Datenschutzverordnung (DSVO) abgeleitet worden sind.

---

[247] Berufsgenossenschaftliche Vorschriften für Sicherheit und Gesundheit bei der Arbeit (BGV).
[248] § 72 Abs. 2 FeV.
[249] § 72 Abs. 1 FeV.
[250] Näheres zum Bioland-Siegel unter http://www.bioland.de/erzeuger/.
[251] § 4 Abs. 2 LDSG i. V. m. der Gütesiegelverordnung.
[252] §1 Abs. 1 und 3 DSAVO.
[253] Abrufbar unter: http://www.datenschutzzentrum.de/gesetze/.

Der Hersteller (oder die Vertriebsfirma) eines IT-Produktes schließt zunächst mit einem oder mehreren beim ULD Schleswig-Holstein akkreditierten Sachverständigen oder Prüfstellen einen privaten Begutachtungsvertrag ab. Meist wird es sich um mehrere Sachverständige handeln, die das Produkt zum einen aus rechtlicher, zum anderen aus technischer Sicht begutachten. Die Sachverständigen prüfen, ob das IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht. Dabei muss zunächst das für das Produkt einschlägige Anforderungsprofil als Soll-Vorstellung aus den Rechtsnormen abgeleitet werden, bevor anschließend auf der Basis der Produktbeschreibung der Ist-Zustand der tatsächlichen Umsetzung festgestellt wird. Beim Prüfansatz ist zu berücksichtigen, dass nicht nur diejenigen Dinge, die das Produkt leisten muss (positive Anforderungen), zu begutachten sind, sondern auch diejenige Funktionalität, die das Produkt nicht beinhalten darf (negative Anforderungen).

Die Sachverständigen legen die Ergebnisse ihrer Prüfung in einem umfassenden Gutachten nieder. Fällt das Gutachten positiv aus, kann der Hersteller unter Vorlage des Gutachtens beim ULD Schleswig-Holstein einen Antrag auf Erteilung eines Gütesiegels stellen. Das ULD überprüft, ob das Gutachten schlüssig und nachvollziehbar ist. Auch können ergänzende Angaben und die Vorlage des IT-Produktes bei Bedarf zusätzlich angefordert werden. Nach erfolgreicher Prüfung vergibt das ULD das Gütesiegel.

Das vergebene Siegel soll den anbietenden Unternehmen wie den Erwerbern Kostenvorteile bringen und ihnen einen Vorsprung am Markt einräumen. In § 4 Absatz 2 LDSG-SH wird von öffentlichen Stellen die vorrangige Verwendung solcher Produkte gefordert, die mit den Vorschriften über den Datenschutz und die Datensicherheit vereinbar sind. Das ULD führt – jeweils online abrufbar – ein Register der anerkannten Sachverständigen nach § 3 Abs. 3 DSAVO[254] sowie eine Übersicht der verliehenen Gütesiegel[255].

5.2.1.4.2 Datenschutzgütesiegel Bremen

Im Oktober 2004 ist die Bremische Datenschutzauditverordnung (BremDSAuditV) [256] in Kraft getreten. Danach können öffentliche Stellen zur Verbesserung des Datenschutzes und der Datensicherheit ihre Verfahren oder technischen Einrichtungen durch einen unabhängigen externen Gutachter prüfen und bewerten lassen. Dieser muss vom Bremer Landesbeauftragten für Datenschutz und Informationsfreiheit zugelassen werden, wobei die Zulassung nur bezogen auf das jeweils zu prüfende Verfahren erteilt wird. Eine generelle Anerkennung von Sachverständigen, wie sie in der schleswig-holsteinischen Datenschutzauditverordnung vorgesehen ist, erfolgt nicht. Der Gutachter prüft den von der öffentlichen Stelle zu erstellenden Datenschutzplan, der auch die Ziele des Datenschutzes und der Datensicherheit umfasst, auf Vollständigkeit und Schlüssigkeit. Die Ziele des Datenschutzes und der Datensicherheit haben sich am „Stand der Technik“ zu orientieren. Bestätigt der Auditor die Vollständigkeit und Schlüssigkeit des Datenschutzplans, so ist die öffentliche Stelle

[254] Abrufbar unter http://www.datenschutzzentrum.de/guetesiegel/registga.htm.
[255] Abrufbar unter http://www.datenschutzzentrum.de/guetesiegel/register.htm.
[256] Abrufbar unter http://www.datenschutz-bremen.de/pdf/Gesetzblatt_2004_53%20BremDSAuditVO.pdf.

für einen Zeitraum von zwei Jahren berechtigt, das Bremische Datenschutzaudit-Gütesiegel für das auditierte Verfahren zu verwenden[257]. Weitere Einzelheiten sind in der Durchführungsbestimmung zur Bremischen Datenschutzauditverordnung geregelt[258]. Für Unternehmen der Privatwirtschaft besteht keine Möglichkeit, das Gütesiegel zu erhalten.

5.2.1.4.3 Grundschutzzertifikat des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI)

Unternehmen können ihre IT-Infrastruktur beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizieren lassen und ein IT-Grundschutz-Zertifikat erhalten.[259] Durch ein IT-Grundschutz-Zertifikat wird nachgewiesen, dass im betrachteten Verbund IT-Grundschutz erfolgreich umgesetzt worden ist. Grundlage für die Vergabe eines solchen Zertifikats ist die Durchführung eines Audits durch einen externen, durch das BSI zertifizierten Auditor. Das Ergebnis des Audits ist der Auditreport, der der Zertifizierungsstelle vorgelegt wird, die über die Vergabe des IT-Grundschutz-Zertifikats entscheidet. Kriterienwerke des Verfahrens sind die IT-Grundschutzkataloge sowie die BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise. Seit 2006 ist die ursprüngliche Zertifizierung nach IT-Grundschutz durch eine anerkannte ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz vollständig abgelöst worden.[260] Bei einer ISO 27001 Zertifizierung auf der Basis von IT-Grundschutz werden neben dem IT-Sicherheitsmanagement auch die konkrete Umsetzung von IT-Sicherheitsmaßnahmen auf der Basis von IT-Grundschutz geprüft. Das Audit wird nach dem Dokument „Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Prüfschema für ISO 27001-Audits“ durchgeführt.[261].

Das BSI vergibt das auf der Grundlage eines positiven Auditor-Votums nach eigener Prüfung das „IT-Grundschutz-Zertifikat“[262]. Der Erwerb des Grundschutzzertifikats ist freiwillig. Das vergebene Siegel soll den anbietenden Unternehmen wie den Erwerbern Kostenvorteile bringen und ihnen einen Vorsprung am Markt einräumen. Das BSI führt ein Register der zertifizierten Prüfstellen[263] und der zertifizierten und mit Grundschutzzertifikat versehenen Unternehmen[264]. Beide Register sind über das Internet unentgeltlich einsehbar.

5.2.2 Niederlande

5.2.2.1 Allgemeines

In den Niederlanden wird die Konformitätsbewertung sowohl in dem geregelten als auch im ungeregelten Bereich als Staatsaufgabe angesehen.[265] Der niederländische Staat fördert zur Stärkung

---

[257] § 7 BremDSAuditV.
[258] Abrufbar unter http://www.datenschutz-bremen.de/pdf/dfaudit.pdf.
[259] http://www.bsi.bund.de/gshb/zert/index.htm.
[260] Vgl. http://www.bsi.bund.de/gshb/zert/ISO27001/schema.htm.
[261] Weitere Ausführungen unter. http://www.bsi.de/gshb/zert/index.htm.
[262] Vgl. http://www.bsi.de/gshb/zert/ISO27001/Pruefschema06.pdf.
[263] Vgl.: http://www.bsi.bund.de/zertifiz/zert/pruefst.htm, http://www.bsi.de/gshb/zert/veroeffentl/auditor.htm und http://www.bsi.de/gshb/zert/veroeffentl/auditor27001.htm.
[264] Vgl. http://www.bsi.de/gshb/zert/veroeffentl/gszertifikate.htm und http://www.bsi.de/gshb/zert/veroeffentl/iso27001_zertifikate.htm.
[265] Röhl, Konformitätsbewertung in Deutschland, S. 86 f.

der Markttransparenz die gesamte Zertifizierungsinfrastruktur. Für beide Bereiche ist die einheitliche Akkreditierungsstelle Raad voor Accreditatie (RvA) zuständig, die im öffentlichen Sektor angesiedelt ist[266]. Ihre Zuständigkeit ist im geregelten Bereich eine ausschließliche, im ungeregelten Bereich steht sie im Wettbewerb mit anderen Akkreditierungsdienstleistern[267]. Die Akkreditierung der Zertifizierer beim RvA erfolgt sowohl im ungeregelten wie im geregelten Bereich auf der Grundlage privatrechtlicher Verträge[268]. Zertifizierungen sind im ungeregelten Bereich freiwillig im geregelten Bereich zum Teil freiwillig (Aufsichtsbereich), zum Teil verpflichtend (Zulassungsbereich). Das Verfahren der Akkreditierung richtet sich nach dem „Reglement voor Accreditatie“[269]. Die Konformitätsbewertungsstellen müssen über eine dokumentierte Struktur verfügen, die ersichtlich macht, dass ihre Unparteilichkeit geschützt ist[270].

5.2.2.2 Beispiele

Für den geregelten Bereich sind für die Niederlande Besonderheiten nicht feststellbar. Als Beispiel für eine Zertifizierung sowohl im geregelten als auch im ungeregelten Bereich sei die Zertifizierung durch SKAL, die Zertifizierungsagentur für Produkte des Bio-Landbaus angeführt, die vom RvA für die Zertifizierung von Biolandbauprodukten in beiden Bereiche zugelassen ist[271]. Staatlich vorgegebene Zertifizierungsschemata oder -vorgaben im ungeregelten Bereich konnten für die Niederlande nicht festgestellt werden.

Im Datenschutzbereich hat die niederländische Datenschutzbehörde Leitlinien für eine Datenschutzauditierung herausgebracht, die von den Unternehmen auf freiwilliger Basis durchgeführt werden kann[272].

5.2.3 United Kingdom

5.2.3.1 Allgemeines

Die Politik der englischen Konformitätsbewertung ist in einem offiziellen Papier des Ministeriums für Handel und Industrie niedergelegt[273]. Die Konformitätsbewertung (nämlich: durch Zertifizierung) soll durch die Marktnachfrage für zertifizierte Produkte und Dienstleistungen und nur bei Erforderlichkeit durch Bestimmungen im öffentlichen Interesse organisiert sein. Sie soll dabei möglichst auf vertraglicher Grundlage und im Wettbewerb der Zertifizierungsstellen untereinander erfolgen. Einzige Akkreditierungsstelle des öffentlichen Bereichs ist der United Kingdom Accreditation Service (UKAS). UKAS ist eine private, nicht gewinnausschüttende Unternehmung mit beschränkter Haftung[274]. Zertifizierungen werden insbesondere als Instrument für die Erschließung neuer Märkte

---

[266] Vgl. http://www.rva.nl/?lng_code=en, dort unter „About the RvA“.
[267] Ein Wettbewerber ist der Centrale Accrediterings Raad, (CAR), vgl. http://www.accreditatie.com/.
[268] Röhl, Konformitätsbewertung in Deutschland, S. 300.
[269] http://www.rva.nl/uli/?uli=AMGATE_10218_1_TICH_L30485458.
[270] Röhl, Konformitätsbewertung in Deutschland, S. 300.
[271] Vgl. http://www.skal.nl/Engels/LinkjesUK/Accreditation.htm, Zertifikate nach EG-Landbauverordnung 2092/91 und privatrechtliche (markenbasierte) Zertifikate.
[272] Der Leitfaden ist abrufbar unter: http://www.dutchdpa.nl/downloads_audit/PrivacyAuditFramework.pdf?refer=true&theme=purple.
[273] „Conformity Assessment Policy in the UK“, vgl. unter http://www.dti.gov.uk/files/file36861.pdf.
[274] http://www.ukas.com/about_ukas/.

ausgewiesen. Über die akkreditierten Organisationen und über die von diesen zertifizierten Unternehmen wird ein Register geführt, das im Internet[275] eingesehen werden kann. Der Zugang zum Register der akkreditierten Unternehmen ist frei, der Zugang zum Register der von diesen zertifizierten Unternehmen erfordert eine besondere Subskription, für die ein Jahresentgelt[276] verlangt wird.

5.2.3.2 Beispiele

Nach dem beschriebenen Konzept sind die Gegenstände der Zertifizierungen sehr vielfältig. So kann ein nationales Schema der Nahrungsmittelsicherheit ebenso auditiert und zertifiziert werden[277], wie auch z. B. die Tätigkeit als „PRINCE2-Projektmanager“[278]

Im Bereich Datenschutz ist eine Zertifizierung der Tätigkeit als Auditor und Zertifizierer nach Art. 51 (7) des Data Protection Act 1998 (DPA-UK) möglich[279]. Art. 51 Abs. (7) DPA-UK bestimmt: „The Commissioner may, with the consent of the data controller, assess any processing of personal data for the following of good practice and shall inform the data controller of the results of the assessment.“ Was in diesem Zusammenhang als „good practice“ zu gelten hat, ist im „Data Protection Audit Manual“ des UK Data Commissioners festgelegt[280]. Datenschutzzertifizierungen können von privaten Zertifizierern auf der Grundlage der Normenreihe ISO 27001 vorgenommen werden; in diesem Rahmen kann auch das Audit-Manual des Commissioners[281] Berücksichtigung finden.

5.2.4 Frankreich

5.2.4.1 Allgemeines

Es gibt zur Akkreditierung in Frankreich eine Vielzahl von Fachgesetzen, jedoch kein übergreifendes Akkreditierungsgesetz. Einzige nationale Akkreditierungsstelle und gleichermaßen für den geregelten wie den ungeregelten Bereich zuständig ist das Comité Francais d'Accreditation (COFRAC)[282]. COFRAC ist als Verein organisiert. Es gibt daneben in größerem Umfang Zertifizierungen ohne entsprechende Akkreditierung bei COFRAC, auch im harmonisierten Bereich[283]. Die Zertifizierungen erfolgen auf der Grundlage von Fachgesetzen oder ministeriellen Erlassen.

---

[275] http://www.quality-register.co.uk/.
[276] Siehe unter http://www.quality-register.co.uk/.
[277] Produktzertifizierung nach ISO 45011, vgl. etwa das „Red Tractor food assurance scheme“, vgl. dazu unter http://www.ukas.com/business/indirect/red_tractor_food_assurance_scheme.asp.
[278] PRINCE2 ist eine in Großbritannien weit verbreitete Projektmanagement-Methode, vgl. http://www.apmgroup.co.uk/web/site/AboutUs/QualityAssurance.asp.
[279] http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm.
[280] Vgl. unter http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/data_protection_complete_audit_guide.pdf, Seite 1.3.
[281] Abrufbar unter http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/data_protection_complete_audit_guide.pdf.
[282] Vgl. unter http://www.cofrac.fr/.
[283] Vgl. Röhl, Konformitätsbewertung in Deutschland, S. 93.

5.2.4.2 Beispiele

Für den geregelten Bereich sind im Gegensatz zu dem ungeregelten Bereich für Frankreich Besonderheiten nicht feststellbar. Im ungeregelten Bereich sind freiwillige Zertifizierungen nach staatlich vorgegebener Auditierungs- und Zertifizierungsschemata für Verbraucherprodukte (Nonfoodprodukte und Dienstleistungen) gemäß Art. L115-27 Code de la Consommation (CdC) in Verbindung mit den einzelnen Fachgesetzen vorgesehen[284]. Ein administrativ vorgegebenes Zertifizierungsschema oder entsprechende Vorgaben im ungeregelten Bereich sind für Frankreich für den Bereich des Datenschutzes in der Planung.

5.2.5 Österreich

5.2.5.1 Allgemeines

In Österreich gibt es ein nationales Akkreditierungsgesetz des Bundes (AkkG)[285]. Regelungen in Fachgesetzen des Bundes (etwa im Medizinproduktegesetz) gehen ihm vor[286]. Für die Akkreditierung nach dem Akkreditierungsgesetz finden die Standards der Normenreihe ISO 17001 ff. Anwendung, ohne dass das Gesetz auf diese Normenreihe verweist[287]. Es besteht eine einzige staatliche Akkreditierungsstelle beim Bundesministerium für Wirtschaft und Arbeit (BMWA), die sowohl für den geregelten als auch den ungeregelten Bereich zuständig ist[288] und die einschlägigen internationalen Abkommen schließt[289]. Zertifizierungsstellen werden nach § 17 Abs. 1 AkkG akkreditiert[290]. Voraussetzungen einer Akkreditierung ist u. a. die Unabhängigkeit der Stelle, die Qualifikation des Personals, die technische und räumliche Ausstattung sowie bestimmte Anforderungen an das Qualitätsmanagementsystem[291]. Das BMWA gibt hierzu Leitfäden heraus, die u. a. auf die ISO-Standards der Konformitätsbewertung in einer vom Ministerium besonders bearbeiteten Fassung verweisen[292]. Auf eine Akkreditierung als Zertifizierungsstelle besteht auch bei Vorliegen der Voraussetzungen kein Anspruch[293]. Die Akkreditierungsstelle beim BMWA führt ein Register der Zertifizierungsstellen getrennt nach Produkten, Managementsystemen und Personal[294].

5.2.5.2 Beispiele

Für den geregelten Bereich sind für Österreich Besonderheiten nicht feststellbar.

---

[284] Vgl. Buch I Titel 1, Kapitel 5 CdC; Das Gesetz ist abrufbar unter: http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006069565&dateTexte=20090405.
[285] Abrufbar unter: http://www.bmwfj.gv.at/NR/rdonlyres/695E086F-1829-4E73-AA82-610B5D44D8CA/0/AkkreditierungsgesetzDeutsch.pdf.
[286] § 1 Abs. 2 S. 1 AkkG.
[287] Röhl, Konformitätsbewertung in Deutschland, S. 309.
[288] Röhl, Konformitätsbewertung in Deutschland, S. 314.
[289] Daneben gibt es für Bauprodukte (Materie des Landesrechts) eine gemeinsame Akkreditierungsstelle der Länder, die für diesen Bereich einheitlich zuständig ist und die fraglichen internationalen Abkommen schließt.
[290] Daneben gibt es die Akkreditierung (nicht zertifizierender) Prüf- und Überwachungsstellen nach § 9 Abs. 1 AkkG.
[291] §§ 18 bis 21 AkkG
[292] http://www.bmwa.gv.at/BMWA/Schwerpunkte/Unternehmen/Akkreditierung/Downloads/default.htm.
[293] § 17 Abs. 5 AkkG.
[294] http://www.bmwa.gv.at/BMWA/Schwerpunkte/Unternehmen/Akkreditierung/ListAkkredStelle/default.htm.

Das Vergeben entsprechender Gütesiegel ist auch für den staatlich ungeregelten privaten Bereich von einer staatlichen Erlaubnis abhängig[295]. Staatlich vorgegebene Zertifizierungsschemata oder -vorgaben im ungeregelten Bereich konnten für Österreich nicht festgestellt werden.

5.2.6 Schweiz

5.2.6.1 Allgemeines

In der Schweiz existiert die Verordnung über das schweizerische Akkreditierungssystem und die Bezeichnung von Prüf-, Konformitätsbewertungs-, Anmelde- und Zulassungsstellen (Akkreditierungs- und Bezeichnungsverordnung, AkkBV)[296]. Akkreditierungen erfolgen durch die staatliche Schweizerische Akkreditierungsstelle SAS[297], die dem Wirtschaftsministerium nachgeordnet ist.

5.2.6.2 Beispiele

Für den geregelten Bereich sind für die Schweiz Besonderheiten nicht feststellbar.
In dem Bereich Datenschutz bestimmt das DSG, dass zur Verbesserung des Datenschutzes und der Datensicherheit Hersteller von Datenbearbeitungssystemen oder -programmen sowie private Personen oder Bundesorgane, die Personendaten bearbeiten, ihre Systeme, Verfahren und ihre Organisation einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen können. Das Gesetz verpflichtet den Bundesrat, Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens zu erlassen sowie dabei das internationale Recht und die international anerkannten technischen Normen zu berücksichtigen[298]. Dem ist der Gesetzgeber durch Erlass der Verordnung über die Datenschutzzertifizierungen (VDSZ) nachgekommen[299].

Zertifizierbar sind nach dieser Verordnung Produkte, die hauptsächlich der Bearbeitung von Personendaten dienen oder bei deren Benutzung Personendaten, namentlich Daten über die Benutzerin oder den Benutzer, generiert werden. Gegenstand der Prüfung ist die produktimmanente Gewährleistung:

- von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der bearbeiteten Personendaten im Hinblick auf den Verwendungszweck des Produkts;
- der Vermeidung der im Hinblick auf den Verwendungszweck des Produkts nicht erforderlichen Generierung, Speicherung oder anderen Bearbeitung von Personendaten;
- von Transparenz und Nachvollziehbarkeit der automatisierten Bearbeitung von Personendaten, die im Rahmen der vom Hersteller festgelegten Funktionalität eines Produkts erfolgt;
- von technischen Maßnahmen zur Unterstützung des Anwenders oder der Anwenderin bei der Einhaltung weiterer Datenschutzgrundsätze und datenschutzrechtlicher Pflichten.

---

[295] Vgl. § 1 der österreichischen Gütezeichenverordnung.
[296] Abrufbar unter: http://www.admin.ch/ch/d/sr/9/946.512.de.pdf.
[297] Vgl. http://www.seco.admin.ch/sas/index.html?lang=de, Einzelheiten dazu Röhl, Konformitätsbewertung in Deutschland, S. 99.
[298] Art. 11 DSG.
[299] Abrufbar unter http://www.admin.ch/ch/d/as/2007/5003.pdf.

Weiter ist in der Verordnung festgelegt, dass er oder die Datenschutzbeauftragte bis spätestens am 1. Januar 2010 Richtlinien darüber erlässt, welche datenschutzspezifischen Kriterien im Rahmen der Zertifizierung eines Produkts mindestens zu prüfen sind[300]. Durch die Zertifizierung ergeben sich nach dieser Vorschrift verminderte datenschutzrechtliche Meldepflichten: Auf Antrag kann von der Pflicht zur Anmeldung von Datensammlungen nach Art. 11a Ab. 5f DSG befreit werden[301]. Der oder die Beauftragte veröffentlicht ein Verzeichnis der Stellen, die eine Zertifizierung erhalten haben und von der Pflicht zur Registrierung ihrer Datensammlungen befreit sind[302]. Staatlich vorgegebene Zertifizierungsschemata oder -vorgaben im ungeregelten Bereich konnten für die Schweiz nicht festgestellt werden.

5.2.7 EuroPriSe: Das Europäische Datenschutzgütesiegel

Das europäische Datenschutzgütesiegel wird auf Antrag an Hersteller von IT-Produkten (z. B. Hard- und Software) und Anbieter IT-basierter Dienstleistungen (z. B. Auftragsdatenverarbeitung oder webbasierte Dienstleistungen wie Online-Banking) verliehen, wenn diesen der Nachweis gelingt, dass das Produkt bzw. die Dienstleistung mit europäischem Datenschutzrecht in Einklang steht. Hersteller eines Produkts und Anbieter einer Dienstleistung setzen durch die Beauftragung anerkannter EuroPriSe-Sachverständiger ein zweistufiges Verfahren in Gang: Zunächst wird das Produkt bzw. die Dienstleistung von den beauftragten Sachverständigen auf Konformität mit EU-Datenschutzrecht und Erfordernissen der Datensicherheit hin begutachtet. Attestieren die Experten die Einhaltung aller im Einzelfall relevanten EuroPriSe-Kriterien, wird ihr Gutachten zusammen mit dem Antrag auf Erteilung eines Gütesiegels bei einer unabhängigen Zertifizierungsstelle eingereicht. Die jeweilige Zertifizierungsstelle überprüft sodann in einem zweiten, die Qualität der Zertifizierung sichernden Schritt, ob das Gutachten vollständig, schlüssig und nachvollziehbar ist und verleiht in diesem Fall das EuroPriSe-Zertifikat. Auf Wunsch des Herstellers bzw. des Anbieters der Dienstleistung kann die Verleihung des Siegels öffentlich vorgenommen werden. Der Hersteller eines zertifizierten Produkts kann dieses mit dem europäischen Datenschutzgütesiegel bewerben und sich durch dieses Alleinstellungsmerkmal einen Wettbewerbsvorteil gegenüber seinen Konkurrenten am Markt verschaffen.

5.2.8 Ergebnis des Rechtsvergleichs

Der Vergleich hat gezeigt, dass die Durchführung von Audits zum einen eine bewährte, akzeptierte, effektive und vielfach angewandte Methode zur Schaffung von Transparenz und Vertrauen ist. Zum anderen ist festzustellen, dass es eine große Homogenität an Verfahren und Vorschriften gibt. Gerade im Bereich Datenschutz ist es offensichtlich, dass einige Regelungen vorhanden sind, aber trotz bestehendem Bedürfnis es in vielen Ländern und Bereichen an entsprechenden Regeln fehlt oder lediglich Empfehlungen vorhanden sind. Die größten Erfahren in dem Datenschutzbereich sind in Deutschland gemacht worden, auf die im Folgenden aus diesem Grund zurückgegriffen wird.

---

[300] Art. 5 VDZS.
[301] Art. 8 Abs. 1 VDSZ.
[302] Art. 8 Abs. 3 VDSZ.

5.3 Kriterien für eine Auditierung von Biobanken

5.3.1 Vorüberlegungen und Festlegung des Zertifizierungsgegenstandes

Die nachfolgenden Kriterien für die Auditierung von Biobanken betreffen aufgrund der Problematik der Nicht-Anonymisierbarkeit von genetischen Daten (s. unter 2.2.2.2) auch Biobanken, bei denen Daten und Proben nur anonymisiert vorgehalten und / oder nur in dieser Form zu Beforschung herausgegeben werden. Sie fassen (datenschutzrechtliche) Grundsätze vertrauenswürdiger Biobanken zusammen. Dabei wird zur Vereinfachung ausschließlich auf die DSLR als gesetzliche Grundlage verwiesen, die in den nationalen Gesetzen Eingang gefunden hat.

Die Kriterien sind ähnlich wie in dem Kriterienkatalog des Schleswig-Holsteinischen Gütesiegels und dem Anforderungskatalog des europäischen Datenschutzgütesiegels EuroPriSe sortiert. Diese Unterteilung ist nicht zwingend, sie hat sich jedoch in der Praxis bewährt, so dass sie im Folgenden übernommen worden ist. Zum Teil sind einige Anforderungen mehrfach aufgeführt. Dabei werden im Regelfall zunächst die wesentlichen Fragen gestellt, die beantwortet werden müssen und anschließend die zu erfüllenden Kriterien (Vorgaben) schlagwortartig benannt oder Anmerkungen dazu gemacht. Der Kriterienkatalog dient dazu, den Auditor in die Lage zu versetzen, die wesentlichen Kriterien einer vertrauenswürdigen Biobank zu erkennen und prüfen zu können. Der Bereich technischer Datenschutz ist nur kurz dargestellt, da dies eine Schnittstelle zu TP-3 ist.

Vor Feststellung bzw. Festlegung der Anforderungen, die an eine Biobank zu stellen sind, ist eine genaue Festlegung des Zertifizierungsgegenstandes erforderlich. Die genaue Festlegung des Zertifizierungsgegenstandes ist von elementarer Bedeutung für ein Zertifizierungsverfahren, da selbst – vermeintlich – kleine Änderungen des Zertifizierungsgegenstands gravierende Auswirkungen auf die durchzuführende Prüfung und das Prüfungsergebnis haben können. Es ist dabei auch zu verlangen, die Datenflüsse abzubilden und eine erste Analyse der anwendbaren Rechtsvorschriften vorzunehmen. Dabei erfolgt inzident eine Überprüfung des Treuhänders, soweit ein solcher intern eingerichtet wurde. Soweit eine externe Datentreuhänderschaft realisiert ist oder werden soll, sollte diese ebenfalls auditiert werden, wobei diese den gleichen Anforderungen genügen muss und daher diese nicht gesondert im Kriterienkatalog erwähnt wird. Insoweit sind zunächst keine Kriterien zur erfüllen, sondern folgende Feststellungen zu treffen:

- Beschreibung der Biobank, die zertifiziert werden soll, insbesondere Organisation und Einheiten,
- Beschreibung, welche personenbezogenen Daten verarbeitet werden, auch wenn diese anonymisiert werden,
- Darstellung der Datenflüsse,
- Darstellung der zur Anwendung kommenden Rechtsgrundlagen der Datenverarbeitung

Vorgaben / Anmerkungen:
Von großem Nutzen sind hier eine festgelegte Aufbau- und Ablauforganisation, eine Geschäftsmodellbeschreibung sowie SOPs, in denen die Vorgehensweise innerhalb der Prozesse beschrieben ist.

5.3.2 Grundlegende Datenschutzrechtliche Anforderungen

In einem ersten Teilkomplex sind elementare Aspekte der in der Biobank erfolgenden Datenverarbeitung zu untersuchen. Zu prüfen ist an dieser Stelle insbesondere, welche Datenverarbeitungsschritte erfolgen, zu welchen Zwecken dies jeweils geschieht, welche personenbezogenen Daten verarbeitet werden und wer für die Datenverarbeitung verantwortlich ist. Dabei soll ein Überblick über die wesentlichen Aspekte der Datenverarbeitung in der Biobank geliefert werden.

5.3.2.1 Feststellung der in der Biobank erfolgenden Datenverarbeitungsschritte

Frage:

- Welche Datenverarbeitungsschritte entstehen in der Biobank?

Vorgaben / Anmerkungen:

Dabei ist insbesondere der Doppelcharakter der Biobank (Daten- und Probensammlung) zu beachten. Im Regelfall sind folgende Datenverarbeitungsschritte zu beschreiben:

- Erhebung der Daten
  - Datenerhebung
  - Probenerhebung
- Speicherung und Weiterverarbeitung der Daten
  - Datenspeicherung
  - Probenspeicherung
- Weitergaben der Daten
  - Weitergabe der Daten
  - Weitergabe der Probe

Rechtsnorm: Art. 2(b) DSRL.

5.3.2.2 Feststellung des Zweckes jedes Datenverarbeitungsschrittes

Fragen:

- Zu welchen Zwecken werden die Daten verarbeitet?
- Ist dieser Zweck jeweils genau festgelegt?
- Sind Aufnahmekriterien festgelegt?
- Ist die Aufbewahrungsdauer der Daten und Proben festgelegt?
- Zu welchen Zwecken werden die Daten an Dritte offenbart?

Vorgaben / Anmerkungen:

Die Feststellung der Zwecke ist besonderes wichtig, weil die Zweckbindung ein entscheidendes Kriterium für den Spenderschutz ist und Auswirkungen hat auf die zu treffenden Maßnahmen. Eine weite Fassung des Zweckes bedeutet, dass ein Mehr an Transparenz erforderlich ist, d. h. dass die Information und die Einwilligung entsprechend ausgestaltet sein muss.

Rechtsnorm: Art. 6(1) (b) DSRL.

5.3.2.3 Feststellung der personenbezogenen Daten, die in dem jeweiligen Datenverarbeitungsschritt verarbeitet werden

Fragen:

- Welche personenbezogenen Daten werden genau verarbeitet?
    - Daten, die aus der Analyse der Proben, d.h. aus einer genetischen Analyse erhoben werden
    - Daten, die direkt beim Betroffenen erhoben werden
    - Daten, die aus einer Behandlung heraus erhoben werden
    - Daten, die durch Verknüpfungen gewonnen werden

Vorgaben / Anmerkungen:

Hier ist insbesondere zu beachten, dass genetische Daten nicht vollständig zu anonymisieren sind und durch genetische Analysen eine unbegrenzte Anzahl an neuen Informationen gewonnen werden kann.

Rechtsnorm: Art. 2(a) und 8 DSRL[303].

5.3.2.4 Verantwortlichkeiten für den jeweiligen Datenverarbeitungsschritt

Fragen:

- Wer ist für die festgestellten Datenverarbeitungsschritte verantwortlich?
- Ist ein Auftragnehmer beauftragt?
- Ist ein Treuhänder eingeschaltet?

Vorgaben / Anmerkungen:

Aus datenschutzrechtlicher Sicht ist es ein wichtiges Anliegen, klare Verantwortlichkeiten für die Proben und Daten verbindlich festzulegen. Zentraler Anknüpfungspunkt für jede datenschutzrechtliche Bewertung ist die Verantwortlichkeit der jeweiligen Daten verarbeitenden Stelle bzw. Person. Ebenso ist hier zu untersuchen, ob sowohl für die Benutzer eines Produktes als auch für die von der Datenverarbeitung betroffenen Personen ein genügendes Maß an Transparenz gewährleistet ist. Insoweit sind vorhandene Dokumente wie z. B. ein Benutzerhandbuch, SOPs und datenschutzspezifische Informationen, wie sie etwa im Rahmen einer Datenschutzerklärung auf einer Website zur Verfügung gestellt werden, auf ihre Vollständigkeit, Richtigkeit, Verständlichkeit und Aktualität hin zu evaluieren.

Rechtsnorm: Art. 2(d) und Art. 17 (2)-(4) DSRL.

Zur Feststellung, welche Datenverarbeitungsschritte erfolgen, zu welchen Zwecken dies jeweils geschieht, welche personenbezogenen Daten verarbeitet werden und wer für die Datenverarbeitung verantwortlich ist, ist eine entsprechende Festlegung und Dokumentation der Biobank erforderlich. Es bedarf daher einer definierten Aufbau- und Ablauforganisation sowie SOPs, in denen die Rechtsgrundlagen, die Datenverarbeitungsschritte und die Verantwortlichen festgelegt sind.

---

[303] Artikel 29-Datenschutzgruppe, WP 91, Arbeitspapier über genetische Daten, S. 5.

5.3.2.5 Datenvermeidung / Datensparsamkeit

Fragen:

- Ist eine Personenbeziehbarkeit erforderlich?
- Ist die Datenverarbeitung auf das erforderliche Maß in Bezug auf den Zweck begrenzt?
- Ab welchem Zeitpunkt kann eine Anonymisierung bzw. Pseudonymisierung erfolgen?
- Ab wann werden die Daten anonymisiert bzw. pseudonymisiert?
- Wie erfolgt die Pseudonymisierung?
- Wie werden die Pseudonyme geschützt?
- Wie erfolgt eine Verknüpfung der genetischen Daten mit den „sonstigen" Daten?
- Ist die Verknüpfung erforderlich?
- Wie lange werden die Daten aufbewahrt? Entspricht die Aufbewahrungsdauer dem Zweck?
- Wird sichergestellt, dass bei Herausgabe nur die erforderlichen Daten herausgegeben werden?

Vorgaben / Anmerkungen:

Zu prüfen ist hier, ob die Biobank technisch so ausgestaltet ist, dass so wenig personenbezogene Daten wie möglich verarbeitet werden, und ob von vorhandenen Möglichkeiten einer Anonymisierung oder Pseudonymisierung Gebrauch gemacht wird.

Aus der festgelegten Aufbau- und Ablauforganisation und die SOPs ergibt sich, ob die Datenverarbeitung bezogen auf jeden Datenverarbeitungsschritt erforderlich und von der Einwilligung gedeckt ist.

Rechtsnorm: Art. 6 und 7 DSRL.

5.3.2.6 Transparenzpflichten

Fragen:

- Sind die Datenverarbeitungsschritte für die Betroffenen transparent?
- Sind Umfang sowie Art und Dauer der Datenverarbeitung transparent?
- Sind die Datenverarbeitungsschritte für die Mitarbeiter, die mit den Daten umgehen, transparent?
- Werden die Betroffenen über die Biobank, ihre Ziele und ihre Arbeit in verständlicher und erreichbarer Form informiert?
- Werden die Betroffenen darüber informiert, wie Datenschutz und Vertraulichkeit gewährleistet werden?
- Erhält der Spender Informationen über die Speicherart und die Zusammenführung von Daten?
- Werden dem Betroffenen die tatsächlichen und rechtlichen Grenzen des Schutzes sowie die Konsequenzen erklärt, die ein Bruch der Vertraulichkeit für ihn haben kann?
- Wenn eine individualisierte Rückmeldung an den Spender vorgesehen ist: Werden die Betroffenen über die Konsequenzen informiert, die sich aus der Mitteilung bestimmter genetischer Dispositionen an sie selbst auch für die Verwandtschaft ergeben?
- Ist dem Betroffenen der Zweck der Datenverarbeitung und Regeln über Vorhaltung, Nutzung und Weitergabe des Materials transparent?

- Berichtet die Biobank regelmäßig über ihre zurückliegenden und ihre geplanten Vorhaben? Einschließlich der geplanten genetischen Analysen?
- Ist die Finanzierung der Biobank transparent?
- Wenn die Möglichkeit besteht, dass eine Biobank privates oder ausländisches Kapital einwirbt oder mit der Verfolgung kommerzieller Interessen beginnt, sollte dies besonders den Spendern klar vermittelt werden.
- Erklärt die Biobank, ob sie die Daten der Biobank mit den aus der Forschung gewonnenen Daten anreichert?
- Informiert die Biobank über die staatlichen Zugriffsmöglichkeiten?
- Informiert die Biobank über mögliche Offenbarungspflichten (z. B. gegenüber einem Versicherungsunternehmen?)
- Erklärt sie den Umgang mit Forschungserträgen / die Kommerzialisierung von Forschungserträgen?
- Wird Betroffenen müssen über seine Rechte aufgeklärt?
- Sind die Datenschutzmaßnahmen bzw. -erklärung
    - Verständlich?
    - Vollständig?
    - Zugänglich?
    - Aktuell?
- Sind die Datenschutzmaßnahmen früh und breit kommuniziert, soweit dies möglich ist, und nicht ausschließlich an mögliche Spender und Nutzer?

Vorgaben / Anmerkungen:
Hier ist zu untersuchen, ob sowohl für die Benutzer eines Produktes als auch für die von der Datenverarbeitung betroffenen Personen ein genügendes Maß an Transparenz gewährleistet ist. Insoweit sind vorhandene Dokumente wie z. B. SOPs sowie die Datenschutzerklärungen etc. auf ihre Vollständigkeit, Richtigkeit, Verständlichkeit und Aktualität hin zu evaluieren.

5.3.3 Rechtmäßigkeit der Datenverarbeitung der einzelnen Datenverarbeitungsschritte

Hier ist die zentrale Frage nach dem Vorhandensein einer Rechtsgrundlage für jegliche, bei der Benutzung des Zertifizierungsgegenstands erfolgende Verarbeitung personenbezogener Daten zu beantworten.

5.3.3.1 Rechtsgrundlage der Datenverarbeitung

Grundlage der Datenverarbeitung in Biobanken ist immer die Einwilligung, die folgende Kriterien erfüllen muss:

Fragen:
- Ist die Einwilligung hinreichend bestimmt?
- Erfolgt die Einwilligung schriftlich?
- Wie ist die Einwilligung / das Formularwerk ausgestaltet?
- Ist eine Abstufung des Einwilligungsumfangs und des Einwilligungszweckes möglich?
- Hat der Betroffene die Option, Forschungszwecke, Geldgeber und Kooperationspartner allgemein auszuschließen?

- Werden dem Spender eine Auswahloptionen wegen des Umfangs der von ihm erteilten Einwilligung eingeräumt?
- Hat der Spender eine Wahloption hinsichtlich der Rückmeldung individualisierbarer Forschungserkenntnisse?
- Hat der Spender eine Quelle genannt bekommen, in der er sich über die Forschungserträge informieren kann?
- Sind die Betroffenen hinreichend aufgeklärt? Sind in den Einwilligungserklärungen folgende Angaben enthalten?
  - Freiwilligkeit der Teilnahme?
  - Zwecke, Art, Umfang und Dauer der vorgesehenen Nutzung einschließlich vorgesehener genetischer Analysen?
  - Umfang und Bedingungen einer möglichen Weitergabe von Proben und Daten?
  - Verfahren der Rückmeldung von Forschungsergebnissen an den Spender?
  - Hinweise auf mögliche Konsequenzen der Mitteilung von Befunden genetischer Analysen für den Spender und verwandte Angehörige einschließlich möglicher Offenbarungspflichten (z. B. gegenüber Versicherungen)?
  - Erneute Kontaktaufnahme?
  - Art der Speicherung und Zusammenführung von Daten?
  - Anonymisierung oder Pseudonymisierung von Proben und Daten und sonstige flankierende Maßnahmen des Spenderschutzes ?
  - etwaige staatliche Zugriffsmöglichkeiten auf Proben und Daten?
  - das Recht des Spenders auf jederzeitigen Widerruf seiner Einwilligung ohne Sanktionen?
  - das Schicksal von Proben und Daten beim Widerruf und bei Beendigung der Biobank?
  - etwaige kommerzielle Perspektiven der vorgesehenen Forschung und Fragen der Aufwandsentschädigung, Bezahlung?
  - Ziele der Forschung?
  - Herkunft der Finanzmittel?
  - vorgesehene Kooperationspartner?
  - etwaige staatliche Zugriffsmöglichkeiten auf Proben und Daten
- Kann der Spender zur Vertiefung nachlesen, was ihm mündlich erklärt wurde?
- Ist der Spender durch einen Arzt aufgeklärt worden?
- Ist dem Spender wegen seiner Entscheidung eine Bedenkzeit eingeräumt worden?

Vorgaben / Anmerkungen:
Je abstrakter und umfassender der Forschungszweck, desto höhere Anforderungen sind an die fortwährende Information der Betroffenen zu stellen.

Hat die Biobank eine sog. materielle Datentreuhänderschaft eingerichtet, d. h. ist dieser mit der Überwachung der Einhaltung der Anforderungen an die Einwilligung und Aufklärung der Spender beauftragt, ist dies in die Prüfung einzubeziehen.

Rechtsnorm: Art. 7(a), 8 (2) (a), 10 und 11 DSRL.

5.3.3.2 Vereinbarkeit der Datenverarbeitung mit wichtigen Datenschutzzielen

Im Zentrum eines weiteren Teilkomplexes steht die Frage nach der Vereinbarkeit der Datenverarbeitung mit wichtigen Datenschutzprinzipien wie Zweckbindung, Verhältnismäßigkeit und Qualität – sprich Richtigkeit – der Daten.

5.3.3.2.1 Zweckbindung

Fragen:

- Werden die Daten für einen bestimmten zulässigen Zweck erhoben? Welche Zwecke sind dies?
- Zu welchen Zwecken werden die Daten verarbeitet?
- Ist die Aufbewahrungsdauer der Daten und Proben festgelegt?
- Zu welchen Zwecken werden die Daten an Dritte offenbart?
- Werden die Zwecke dokumentiert?
- Werden die Daten zu anderen Zwecken als zu dem ursprünglich erhobenen Zweck verarbeitet? Liegt eine Zweckänderung vor?
- Sind die Verarbeitungsschritte dokumentiert, so dass unzulässige Zweckänderungen erkennbar sind?
- Sind Maßnahmen getroffen, die eine unzulässige Zweckänderung ausschließen?

Vorgaben / Anmerkungen:

Zum Teil wird die Zweckbindung bereits oben erörtert und kann an dieser Stelle kürzer gefasst werden, sie bereits ausführlich behandelt wurde. Auch hier gilt, je abstrakter und umfassender der Forschungszweck, desto höhere Anforderungen sind an die fortwährende Information der Betroffenen zu stellen.

Rechtsnorm: Art. 6 (1) (b) DSRL.

5.3.3.2.2 Verhältnismäßigkeit

Fragen:

- Werden nur die Daten verarbeitet, die zur Erreichung des festgelegten Zwecks erforderlich sind?
- Wann werden die Daten gelöscht?

Vorgaben / Anmerkungen:

Für jeden Schritt der Verarbeitung dieser Daten ist zu prüfen, ob die Verarbeitung zur Erreichung des Forschungszwecks geeignet und notwendig ist und die Eingriffstiefe nicht außer Verhältnis zu dem angestrebten Zweck steht. Eine unbefristete Aufbewahrung ist grundsätzlich unverhältnismäßig.

Rechtsnorm: Art. 6 (1) (c) DSRL.

5.3.3.2.3 Qualität

Frage:

- Werden Vorkehrungen getroffen, um die Integrität der Daten zu gewährleisten?

Vorgaben / Anmerkungen:
Siehe unter Datensicherheit.

Rechtsnorm: Art. 6 (1) (d) DSRL.

5.3.3.3 Rechtmäßigkeit der jeweiligen Datenverarbeitung in jeder Phase

Dieser Teilkomplex hat Kriterien zum Gegenstand, die sich mit der Rechtmäßigkeit spezieller Phasen der Datenverarbeitung befassen. Zu prüfen ist hier beispielsweise, ob die betroffenen Personen bei der Erhebung von Daten ordnungsgemäß informiert werden, ob Daten an Dritte übermittelt werden dürfen oder wann Daten nicht mehr erforderlich und damit zu löschen sind.

5.3.3.3.1 Datenerhebung und -vorhaltung: Ordnungsgemäße Information

Fragen

- Werden die Daten direkt bei dem Betroffenen erhoben oder indirekt, d.h. aus dem Behandlungszusammenhang?
- Erhalten die Betroffenen die für ihre Entscheidung notwendigen Informationen?

Vorgaben / Anmerkungen:
Hier wird auf die Ausführungen bei der Einwilligung verwiesen. Es ist zu beachten, dass diese Anforderungen sowohl bei direkter aus auch indirekter Datenerhebung gilt, da in jedem Fall eine Einwilligung erforderlich ist.

Rechtsnorm: Art. 6 (1) (b) du (c) Art. 7, 10 und 11 DSRL.

5.3.3.3.2 Datenübermittlung an Dritte

Fragen:

- Werden die Daten entsprechend dem vorgegebenen Zweck bzw. entsprechend der Einwilligung übermittelt?
- Erhalten die Betroffenen ausreichende Informationen über die Datenübermittlung?
- Wer erhält die Daten?
- Ist die Daten-/Probenübermittlung protokolliert bzw. dokumentiert?
- Sind nur die erforderlichen Daten übermittelt worden?
- Wird sichergestellt, dass die Daten den richtigen Empfänger erreichen?
- Werden die Proben in anonymisierter Form weitergeleitet?
- Ist die Datenübermittlung auf konkret definierte Empfänger und konkret bezeichnet Forschungsvorhaben beschränkt?
- Wurde der Empfänger verpflichten, die Daten nur für den ursprünglichen Zweck zu verarbeiten, sie nicht an Dritte weiter zu übermitteln und diese nach Abschluss des Forschungsprojektes zu löschen?
- Wird die Herausgabe von Proben an Dritte möglichst vermieden?
- Wird vor einer Veröffentlichung des Forschungsergebnisses das Re-Identifizierungsrisiko geprüft?

- Ist das Forschungsprojekt, das die Daten erhält, ethisch zustimmend bewertet worden?
- Werden Forschungsergebnisse individualisierbar zurückgemeldet?

Vorgaben / Anmerkungen:
Von wesentlicher Bedeutung für den Schutz des Spenders ist ein Material Transfer Agreement mit dem Empfänger, in dem dieser – u. U. unter Vereinbarung einer Vertragsstrafe – auf die Einhaltung der datenschutzrechtlichen Anforderungen verpflichtet wird – u. a. auf die Verarbeitung der Daten entsprechend der Einwilligung des Betroffenen. Es wird ein Weiterübermittlungsverbot vereinbart sowie das Verfahren zum Schutz der Spenderrechte festgelegt.
Nur ethisch zustimmend bewertete Forschungsvorhaben erhalten Daten und Proben.
Werden Daten pseudonymisiert übermittelt, so geschieht dies ausschließlich auf der Grundlage einmalig verwendeter Transaktionspseudonyme.
Eine Übermittlung von Daten und Proben zur Beforschung erfolgt ausschließlich für bestimmte einzelne Studien.
Die empfangene Stelle bestätigt den Erhalt, Verwendung und Löschung der Daten.

Rechtsnorm: Art. 6 (1) (b) und (c), 7, 10, 11, 14 (b), 17 (1) DSRL.

5.3.3.3.3 Datenlöschung

Fragen:

- Wann wird eine Datenlöschung vorgesehen?
- Ist sichergestellt, dass die Daten gelöscht werden, wenn sie zur Erfüllung des ursprünglichen Zwecks nicht mehr erforderlich sind? Wie erfolgt die Sicherstellung?
- Sind Prüf- und Löschfristen vorgesehen?
- Wird die Löschung regelmäßig vollzogen und überprüft?
- Ist eine Sperrung der Daten möglich?

Vorgaben / Anmerkungen:
Eine unbefristete Verwahrung der Proben ist grundsätzlich nicht zulässig.

Rechtsnorm: Art. 6 (1) (e) DSRL.

5.3.3.4 Besondere Arten der Datenverarbeitung sowie besondere Pflichten der Verantwortlichen

Gegenstand des vierten Teilkomplexes sind Kriterien, die die Rechtmäßigkeit spezieller Varianten der Datenverarbeitung wie Auftragsdatenverarbeitung und Übermittlung personenbezogener Daten in Drittländer betreffen, sowie die Verpflichtung des für die Verarbeitung Verantwortlichen zur Meldung einer Datenverarbeitung bei der Kontrollstelle und zur Vorabkontrolle von Verarbeitungen, die spezifische Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können.

5.3.3.4.1 Besondere Arten der Datenverarbeitung

Fragen:

- Sind Dritte in die Datenverarbeitungsschritte eingebunden?
- Ist der Dritte Auftragnehmer oder selbst Verantwortlicher?

- Ist ein Treuhänder eingeschaltet?
- Welche Vereinbarungen sind mit diesem getroffen worden?
- Ist der Treuhänder rechtlich und tatsächlich unabhängig?

Vorgaben / Anmerkungen:
Ist ein Datentreuhänder eingeschaltet, wird dieser, soweit er intern realisiert ist, implizit geprüft. Ist ein externer Datentreuhänder eingeschaltet, sollte dieser sich gleichfalls einer Auditierung unterziehen. Er hat dann gleichermaßen die Kriterien zu erfüllen.

5.3.3.4.2 Meldungen und Vorabkontrolle

Frage:

- Bestehen gesetzliche Meldepflichten?
- Besteht Soft Law, die eine Meldepflicht gebietet?
- Ist eine Vorabkontrolle notwendig?

Rechtnorm: Art. 18, 19 und 20 DSRL.

5.3.4 Technisch-organisatorische Maßnahmen

Der dritte Komplex des Katalogs betrifft die zur Gewährleistung der Datensicherheit von dem für die Verarbeitung Verantwortlichen zu treffenden technisch-organisatorischen Maßnahmen. In einem ersten Teilkomplex werden Kriterien aufgelistet, die generelle Pflichten zum Gegenstand haben. Hierzu zählt etwa die Pflicht zur Kontrolle des Zutritts zu Datenverarbeitungssystemen oder zur Verhinderung einer unbefugten Nutzung solcher Systeme. Außerdem gehören dazu auch die Pflichten zur Protokollierung der Datenverarbeitung, zur Gewährleistung von Netzwerk- und Transportsicherheit und zur Verhinderung eines zufälligen Verlusts von Daten. Die verbleibenden Kriterien dieses Teilkomplexes betreffen technische Aspekte der Löschung von Daten, temporäre Dateien und die Dokumentation von Produkten und Dienstleistungen aus der Perspektive eines Kunden. Gegenstand des zweiten Teilkomplexes sind spezielle, technik- und dienstleistungsspezifische Anforderungen. Die insoweit einschlägigen Kriterien betreffen Themen wie Verschlüsselung, Anonymisierung und Pseudonymisierung sowie die Pflicht zur Gewährleistung der Transparenz automatisierter Einzelentscheidungen.

5.3.4.1 Allgemeine technisch-organisatorische Anforderungen an die Datensicherheit

Um Überschneidungen mit TP-3 zu vermeiden, wird dieser Teil nur kurz und nicht abschließend, sondern lediglich der Vollständigkeit halber behandelt.

Fragen:
Sind Maßnahmen der Datensicherheit getroffen worden, um

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle)?
- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle)?

- 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)?
- 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 Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle)?
- zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle)?
- zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)?
- zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)?
- zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können?

Vorgaben / Anmerkungen:
Es ist die Doppelstruktur die Biobanken zu beachten: Es muss sowohl ein entsprechender Schutz für Daten und Proben gewährleistet werden, welcher der Sensibilität der Daten gerecht werden.

Rechtsnorm: Art. 6 (1) (b) und (c), Art. 7, 10, und 11 DSRL.

5.3.4.2 Spezielle technisch-organisatorische Anforderungen an die Datensicherheit

Fragen:

- Werden die Daten pseudonymisiert?
- Was für ein Pseudonymisierungsverfahren wird verwendet?
- Werden die Daten verschlüsselt?
- Welches Verschlüsselungsverfahren wird eingesetzt?

Vorgaben / Anmerkungen:
Es ist ein abschnittbezogenes Pseudonymisierungsverfahren umzusetzen.
Die Übermittlung von Daten zur Beforschung erfolgt stets nur nach Mehrfach-Pseudonymisierung.
Daten zur Beforschung werden ausschließlich verschlüsselt übermittelt.
Gibt die Biobank für ein Forschungsprojekt Daten nicht anonymisiert, sondern pseudonymisiert heraus, so geschieht dies ausschließlich auf der Grundlage von Transaktionspseudonymen.

5.3.5 Betroffenenrechte

Der vierte Komplex des Katalogs beinhaltet Kriterien, die die subjektiven Rechte der von einer Datenverarbeitung betroffenen Personen zum Gegenstand haben. Der erste Teilkomplex betrifft

subjektive Rechte, die durch die allgemeine Datenschutzrichtlinie garantiert werden. Hierzu gehört zunächst einmal das „Recht auf Information“, welches mit den Pflichten des für die Verarbeitung Verantwortlichen zur Unterrichtung und Benachrichtigung der betroffenen Personen korrespondiert. Die weiteren Kriterien befassen sich mit den Rechten auf Auskunft, Berichtigung, Löschung und Sperrung sowie mit dem Recht, einer Datenverarbeitung in bestimmten Fällen zu widersprechen.

Fragen:

- Ist eine für den Datenschutz und die Datensicherheit verantwortliche Position festgelegt?
- Sind Ansprechpartner für die Betroffenen festgelegt und kommuniziert?
- Haben die Betroffenen das Recht, ohne Angabe von Gründen die Teilnahme an einem Forschungsprojekt zu verweigern?
- Haben die Spender das Recht von der Teilnahme an der Biobank zurückzutreten?
- Kann das Recht auf Widerruf jederzeit ausgeübt werden?
- Gibt es kommunizierte Regeln darüber, wann welche Informationen aus der Forschung zurück in die Biobank gehen und wann solche Informationen an den Spender weiterzuleiten sind?
- Wie wird mit ungesicherten Forschungserträgen umgegangen? Werden sie an den Spender gemeldet?
- Ist die Verfolgbarkeit von Proben und Daten sichergestellt?
- Hat die Biobank erklärt, ob und welche Rechte Spender an Proben und Daten behalten?
- Haben die Betroffenen das Recht, auf individuelle Rückmeldungen zu verzichten?
- Erhalten die Spender vor der Einwilligung eine Bedenkzeit?

Rechtsnorm: Art. 11-13 DSRL.

5.3.6 Qualitätssichernde Maßnahmen

Der letzte Komplex betrifft die qualitätssichernden Maßnahmen. Hier werden Anforderungen an die Prozessorganisation, die Dokumentation und das Datenschutzkonzept gestellt.

5.3.6.1 Prozessorganisation

Für eine professionelle Datenverarbeitung und ihre Prüffähigkeit ist das Aufsetzen und Durchführen aller notwendigen Prozesse erforderlich. Alle Prozesse und Verfahren sind nachvollziehbar und verständlich zu dokumentieren. Teile dieser Dokumentation können in die Informationsmaterialien eingehen, die Betroffenen gegeben werden, die sich für die Datenverarbeitung interessieren. Es sind daher eine Aufbau- und Ablauforganisation sowie SOPs zu definieren, in denen die betrieblichen Prozesse festgelegt sind (vgl. unter 4.2 und 4.3) sowie die Verantwortlichkeiten verbindlich zugewiesen sind.

5.3.6.2 Dokumentation / Datenschutzkonzept

Dokumentationen sind die Voraussetzungen der Prüffähigkeit einer Biobank, einer Selbstbindung, für die Sicherung der Betroffenenrechte, zur Erfüllung der Transparenzpflichten sowie Grundlage von organisatorischen Maßnahmen zur Datensicherheit. Die oben genannten Anforderungen, die in den ersten vier Komplexen angeführt sind, müssen im Ergebnis Bestandteil der Dokumentationen sein. Die Biobank muss daher ein Datenschutzkonzept vorhalten, das die folgenden Dokumente umfassen sollte:

- **Datenflussdiagramm**

Es ist ein Datenflussdiagramm zu erstellen.

- **Geschäftsmodellbeschreibung**

Sie enthält allgemeine Informationen über die Geschäfte der Biobank, die nicht zwingend Bestandteil der Einwilligung werden muss. Sie bezieht sich auf ihre Biobank-Forschung allgemein. Der Spender muss nicht nur bei Einwilligung, sondern fortlaufend über die Geschäfte informiert werden können. Die Geschäftsmodellbeschreibung sollte die unter 4.5 skizzierten Inhalte haben.

- **SOPs**

Die Biobank nimmt für die operative Gestaltung ihrer internen Abläufe zu Einwerbung, Erhebung, Verarbeitung, Analytik, Aufbereitung und Übermittlung an die Forschung, zur Gewährleistung von Spenderrechten sowie zur Qualitätssicherung eine systematische Bestimmung vor und fixiert diese abschließend in betrieblichen Prozessen. Zugleich werden die Verantwortlichkeiten festgelegt (siehe unter 4.3).

- **Sicherheitskonzept**

Abschließende Darstellung der getroffenen organisatorischen Maßnahmen zur Datensicherheit einschließlich Darstellung des Pseudonymisierungsverfahrens und der Protokollierungen (siehe unter 5.3.4).

- **Jährlicher Datenschutzbericht**

Siehe unter 4.5.3.

- **Konzept des Einsatzes von Datentreuhändern**

D. h. eine Übersicht, die erkennen lässt, an welchen Stellen Datentreuhänder nach welchen Regeln in die Abläufe der Biobank integriert sind und welche Vereinbarungen mit diesem getroffen worden sind.

- **Bzw. Verträge über eine Datenverarbeitung im Auftrag**

Bei Vorliegen einer Datenverarbeitung im Auftrag sind die schriftlichen Vereinbarungen zur Auftragsdatenverarbeitung. vorzuhalten.

- **Ablaufkonzept zur Ausübung von Spenderrechten**

Eine Übersicht zum Ablaufkonzept zur Ausübung von Spenderrechten, die ausweist, wie Auskunftsansprüche der Betroffenen erfüllt werden und wie deren Ansprüche auf Löschung, Berichtung und Widerruf nachgekommen wird. Soweit hierbei externe Datentreuhänder eingesetzt werden, sind auch die diesbezüglichen Abläufe und die insoweit bestehenden Vorkehrungen zur Sicherstellung der Datensparsamkeit zum Schutz der Vertraulichkeit der Identität des Spenders dargelegt.

- **Muster einer Spenderaufklärung und –einwilligung**
- **Eine Verzeichnis der informationstechnischen Geräte, Verfahren und Programme**

5.3.6.3 Kontrollmöglichkeiten / Prüfungen

Es sind sowohl angemeldete als auch unangemeldete Überprüfungen des Betriebs notwendig, um das Datenschutz- und IT-Sicherheitsniveau dauerhaft auf hohem Niveau zu gewährleisten. Voraussetzung jeder Prüfung ist die Dokumentation und – auf technischer Ebene – die Protokollierung.

5.3.6.4 Automatisiertes bzw. prozessorientiertes Datenschutzmanagement

Die Umsetzung der Anforderungen des Datenschutzes und der Datensicherheit soll technisch unterstützt und in die Prozesse der Biobank integriert werden.

6 Zusammenfassung und Empfehlungen

Die Forschung mit menschlichem Material sowie die Sammlung und Vorhaltung von entsprechenden Proben und Daten in Biobanken ist aufgrund der besonderen Risiken für die Spender nur zu verantworten, wenn ausreichende Schutzmaßnahmen getroffen sind. Die Datentreuhänderschaft ist eine Möglichkeit, den Schutz der Betroffenen effektiv umzusetzen. Das Institut der Treuhänderschaft wird zwar verschiedentlich als Vorkehrung zum Schutz der Betroffenen genannt. Allerdings fehlen detaillierte Angaben, auch gibt es noch keine allgemeine gesetzliche Regelung. Die vorhandenen detaillierten gesetzlichen Vorgaben betreffen den Sozialversicherungsbereich sowie die medizinische Krebsforschung. Dort sind zum Schutz der Betroffenen Vertrauensstellen gesetzlich eingerichtet worden, die die personenbezogenen Daten pseudonymisieren und „verwalten“, so dass die forschenden oder sonstigen Einheiten, die die Daten nutzen, lediglich pseudonymisierte Daten erhalten. Eine Zusammenführung der Daten ist nur in den gesetzlichen vorgesehen Fällen und nach einem bestimmten Verfahren möglich. Die Vertrauensstellen unterliegen als öffentliche Einrichtungen in der Regel besonderem öffentlichen Schutz, z. B. indem im Sozialbereich der Sozialdatenschutz Anwendung findet oder indem medizinischen Bereich, die Einrichtung ärztlicher Leitung unterstellt wird. Bisher existiert nur in Hamburg eine gesetzlich Regelung, die ausdrücklich Vorgaben für Biobanken enthält, dabei jedoch ausschließlich für Hamburger krankenhausinterne Biobanken gilt.

Das Modell des externen Datentreuhänders ist aber nur bedingt auf die Biobank-Forschung anwendbar, da die notwendige rechtliche, finanzielle und organisatorische Unabhängigkeit grundsätzlich nur durch gesetzliche Regelungen und entsprechend gesicherte finanzielle Ausstattung hergestellt werden kann, die im privaten Biobankgeschäft schwerlich herzustellen ist. Hinzu kommt, dass ein entsprechender Datentreuhänder eine Probenerhebungs- und -vorhaltungsinfrastruktur haben müsste, um nicht nur mit den Daten, sondern auch mit den Proben umgehen zu können. Dies ist praktisch nur schwer umsetzbar. Es ist daher eine Modifizierung des Datentreuhändermodells nötig: Dieser wird innerhalb der Organisation selbst und eingerichtet und muss unaufgefordert bestimmten Transparenzpflichten nachkommen.

Nicht nur, aber auch wegen der Reduzierung der Schutzfunktion eines externen Treuhänders sind weitere Maßnahmen des Spenderschutzes zu treffen. Eine besondere Rolle kommt, solange es keine gesetzlichen Regelungen gibt, der Selbstregulierung zu. Biobanken sollten und müssten ihre Aufbau- und Ablauforganisation festlegen und dabei den Datenschutz und die Datensicherheit integrieren. Mittels SOPs sollte intern eine verbindliche Festlegung auf einen datenschutzkonformen und die Persönlichkeitsrechte der Betroffenen schützenden Umgang mit den Daten und Proben vorgenommen werden. Mittels Festlegung von Verhaltensregeln – Codes of Conduct – sollte sich die „Gemeinschaft der Biobank-Forschung“ entsprechend dem Vorbild der börsennotierten Unternehmen selbst auf die Einhaltung datenschutzrechtlicher Anforderungen verpflichten.

Von besonderer Bedeutung ist außerdem die Transparenz der Biobank für die Öffentlichkeit. Mittels für die Öffentlichkeit bestimmte Geschäftsmodellbeschreibungen, Datenschutz-Policies, durch die Veröffentlichung der Spenderaufklärungen und –einwilligungen sowie eines jährlichen Datenschutzberichtes kann die erforderliche Transparenz hergestellt werden.

Zuletzt sollte eine Standardisierung der Anforderungen vorangetrieben und Auditierungen angeboten und vorgenommen werden. Auditierungen gewährleisten in besonderem Maße Rechtsicherheit für den Betreiber und die Betroffenen und können so beiden Seiten erhebliche Vorteile bringen.

Nichtsdestotrotz bleibt der Gesetzgeber aufgefordert, die bisher unbefriedigende Rechtslage durch eine spezialgesetzliche Regelung zu verbessern. Im Interesse der Rechtssicherheit aller Beteiligten müssen Anforderungen, die sich in den nationalen und internationalen Diskussionen herausgebildet haben und die sich aus dem grundrechtlichen Schutz der Persönlichkeit ergeben, gesetzlich festgelegt werden. Solange es keine Präzisierung des Einwilligungserfordernisses, der Notwendigkeit von Beratung und Aufklärung oder des Rechts auf Nichtwissen gibt, können diese elementaren Sicherungen im Zweifel ignoriert werden. Der notwendige Aufklärungsumfang und die zwingenden Inhalte und das Verfahren einer Einwilligung müssen gesetzlich festgeschrieben werden.

Dabei geht es aber nicht nur um die Festschreibung gefestigter Rechtspositionen, sondern es müssen weiterreichende Vorkehrungen getroffen werden, um die Selbstbestimmung der Menschen zu wahren. Dazu gehört, dass zur Verhinderung eines unzulässigen Umgangs mit menschlichem Material eine Strafnorm geschaffen werden sollte, mit der sowohl ein gesetzgeberisches Unwerturteil zum Ausdruck kommt als auch eine effektive Ahndungsmöglichkeit geschaffen wird.

Regelungsbedarf gibt es hinsichtlich der Genehmigungs- bzw. Anzeigepflicht von Biobanken. Entsprechend den bereits in anderen Ländern bestehenden Regelungen sind eine Genehmigung bzw. die Anzeige von Biobanken sowie ein öffentliches Register, in denen die sich die Spenderinnen und Spender ebenso wie die allgemeine Bevölkerung über die Biobanken sowie die mit der Biobank verbundenen oder ermöglichten Forschungsprojekte informieren kann, unabdingbar.

Darüber hinaus müsste auch eine Absicherung der in den Biobanken vorgehaltenen Daten durch die Einführung eines Forschungsgeheimnisses vorgenommen werden. Es muss ein entsprechender Schutz gewährleistet werden, wie es im Sozialbereich durch den Sozialdatenschutz oder durch die ärztliche Schweigepflicht erreicht wird. Jedenfalls soweit es um die Verarbeitung von genetischen Daten geht, muss wegen der dargestellten Gefahrenlage Entsprechendes vorgesehen werden.

Zuletzt ist eine Verhinderung diskriminierender bzw. missbräuchlicher Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versicherungsverhältnis durch ein grundsätzliches Verbot, Gentests oder Testergebnisse zu fordern oder sie auch nur entgegenzunehmen, erforderlich. Letztere Forderung ist durch das Gendiagnostikgesetz bereits umgesetzt.