

Berliner Beauftragter für Datenschutz
und Informationsfreiheit

Hessischer Datenschutzbeauftragter

**Datenschutz
in
Wissenschaft und Forschung**

Rainer Metschke

Rita Wellbrock

Impressum

Herausgeber:

Berliner Beauftragter für
Datenschutz und Informationsfreiheit
Verantwortlich: Volker Brozio
Redaktion: Laima Nicolaus

Pallasstraße 25/26, 10781 Berlin

Telefon: (0 30) + 75 60 78 09

Telefax: (0 30) 2 15 50 50

E-Mail: mailbox@datenschutz-berlin.de

Internet: <http://www.datenschutz-berlin.de>

Druck:

Druckerei Conrad GmbH

3., überarbeitete Auflage: Dezember 2002

Inhaltsverzeichnis

	Seite
Vorwort	7
1. Verfassungsrechtliche Aspekte	9
1.1 Regelungen für Konflikte zwischen Forschung und Recht auf informationelle Selbstbestimmung	9
1.2 Eingriffe in das informationelle Selbstbestimmungsrecht – Prüfung des legitimierenden Gemeinschaftsinteresses, des Geeignetheitsgrundsatzes, des Erforderlichkeitsgrundsatzes und des Übermaßverbotes	10
1.2.1 Legitimierendes Gemeinschaftsinteresse	10
1.2.2 Geeignetheitsgrundsatz	11
1.2.3 Erforderlichkeitsgrundsatz	11
1.2.4 Übermaßverbot	12
1.3 Übersichtsdarstellung	13
2. Rechtliche Vorgaben der EG-Datenschutzrichtlinie	16
2.1 Zweckdurchbrechung für Zwecke der Forschung	16
2.2 Aufbewahrung für Zwecke der Forschung	17
2.3 Information der Betroffenen	17
2.4 Rechtliche Vorgaben für die Verarbeitung sensibler Daten	17
2.5 Sonstige Regelungen	18
3. Personenbezogene, anonymisierte und pseudonymisierte Daten	19
3.1 Wann sind Daten personenbezogen?	19
3.2 Daten Verstorbener	19
3.3 Anonymisierte Daten	20
3.4 Anonymisierungsverfahren	22
3.5 Pseudonymisierungsverfahren	23
4. Verarbeitung personenbezogener Daten auf der Grundlage einer Einwilligung der Betroffenen	25
4.1 Informierte Einwilligung durch Aufklärung	25
4.2 Zweckbindung durch konkrete Benennung des Forschungsvorhabens	27
4.3 Freiwilligkeit der Einwilligung	28
4.4 Schriftlichkeit der Einwilligung	29

	Seite
4.5 Einwilligung bei nicht einwilligungsfähigen Personen	30
4.5.1 Grundsätzliches	30
4.5.2 Spezialgesetzliche Regelungen	31
4.5.3 Forschung außerhalb der spezialgesetzlich geregelten Bereiche	31
5. Gesetzliche Regelungen zur Forschung mit personenbezogenen Daten ohne Einwilligung der Betroffenen	33
5.1 Grundsätzliches	33
5.2 Rechtliche Vorgaben von Forschungsregelungen am Beispiel von § 30 BlnDSG und § 33 HDSG	33
5.2.1 Konkretes Forschungsvorhaben	34
5.2.2 Wissenschaftliches Forschungsvorhaben	34
5.2.3 Keine Beeinträchtigung schutzwürdiger Belange der Betroffenen	34
5.2.4 Alternativ: Überwiegendes öffentliches Interesse an der Durchführung des Forschungsvorhabens	35
5.2.5 Keine Möglichkeit, den Zweck der Forschung auf andere Weise zu erreichen	36
5.2.6 Zustimmung der obersten Landesbehörde	37
5.2.7 Zweckbindung der Daten	37
5.2.8 Trennungs- und Löschungsgebot	37
5.2.9 Kontrollmöglichkeit	38
5.2.10 Veröffentlichung der Daten	38
5.2.11 Eigenforschung	39
5.2.12 Resümee	39
6. Kombinationsformen des Datenzugangs	40
6.1 Das Adressmittlungsverfahren	40
6.2 Datentreuhänder	41
6.2.1 Die Grundidee	41
6.2.2 Anonymisierung/Pseudonymisierung der Daten durch den Treuhänder	42
6.2.3 Verknüpfung der Daten durch den Treuhänder	42
6.2.4 Datenerhaltung, -bereitstellung und -archivierung durch den Treuhänder	43
6.2.5 Beispiel: Das Projekt QuaSi-Niere	43
7. Spezielle Fragestellungen einzelner Forschungsgebiete	45
7.1 Löschungsgebot wider Sicherung guter wissenschaftlicher Praxis	45
7.2 Neue Probleme bei der Genom-Forschung	46
7.3 Pre-Tests	47
7.4 Personen der Zeitgeschichte sowie Funktions- bzw. Amtsträger	47

7.5	Zeitweilige Beschäftigung von Forschern bei Daten besitzenden Stellen („One-Dollar-Persons“)	48
7.5.1	One-Dollar-Person und das Statistikgeheimnis	50
7.5.2	Ärzte als One-Dollar-Persons und die ärztliche Schweigepflicht	50
7.6	Erweiterter Zugang von Forschern zu Daten der amtlichen Statistik	50
8.	Forschungsregister	51
	Weiterführende Literatur	53
	Anlagen	55
1.	Beispiele für Einwilligungserklärungen	55
	Beispiel 1	56
	Beispiel 2	58
	Beispiel 3	61
2.	Beispiele für Codierungen	63
	Beispiel 1	63
	Beispiel 2	64
3.	Auszüge der in dieser Broschüre eingehend dargestellten Regelungen	65
3.1	Bundesrecht	65
3.1.1	Grundgesetz der Bundesrepublik Deutschland	65
3.1.2	Volkszählungsurteil des Bundesverfassungsgerichts	66
3.1.3	Bundesdatenschutzgesetz	67
3.1.4	Strafgesetzbuch	71
3.2	Berliner Landesrecht	73
3.2.1	Verfassung von Berlin	73
3.2.2	Berliner Datenschutzgesetz (Auszug)	73
3.3	Hessisches Landesrecht	76
3.3.1	Hessisches Datenschutzgesetz (Auszug)	76
4.	Übersicht über weitere Forschungsregelungen	78
4.1	Bund	78
4.1.1	Sozialgesetzbuch X	78
4.1.2	Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz – BStatG)	78
4.1.3	Gesetz über die Sicherung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz – BArchG)	78

	Seite
4.1.4 Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz – BZRG)	78
4.1.5 Strafprozessordnung (StPO)	79
4.1.6 Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz – StUG)	79
4.1.7 Umweltinformationsgesetz (UIG)	79
4.1.8 Straßenverkehrsgesetz	79
4.1.9 Gesetz über die Statistik der Straßenverkehrsunfälle (Straßenverkehrsunfallstatistikgesetz – StVUnfStatG)	79
4.1.10 Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften	79
4.1.11 Strafvollzugsgesetz (StVollzG)	79
4.2 Berlin	80
4.2.1 Berliner Informationsfreiheitsgesetz	80
4.2.2 Meldegesetz Berlin	80
4.2.3 Landesstatistikgesetz	80
4.2.4 Gesetz über die Sicherung und Nutzung von Archivgut des Landes Berlin (Archivgesetz des Landes Berlin – ArchGB)	80
4.2.5 Landeskrankenhausgesetz (LKG)	80
4.2.6 Berufsordnung der Ärztekammer Berlin	80
4.2.7 Bereichsspezifische Regelungen für die Verarbeitung personenbezogener Daten (Artikelgesetz)	81
4.3 Hessen	81
4.3.1 Hessisches Meldegesetz	81
4.3.2 Landesstatistikgesetz	81
4.3.3 Landesarchivgesetz	81
4.3.4 Landeskrankenhausgesetz	81
4.3.5 Hessisches Schulgesetz	81
4.3.6 Hessisches Krebsregistergesetz	82
4.3.7 Berufsordnung für die Ärztinnen und Ärzte in Hessen	82
5. Internationale Vereinbarungen/Rechtsvorschriften/Erklärungen	83
5.1 EG-Datenschutzrichtlinie	83
5.2 Erklärung der European Science Foundation zu der Verwendung personenbezogener Daten zu Forschungszwecken	83
5.3 Europarat-Empfehlung zum Schutz personenbezogener Daten für Zwecke der wissenschaftlichen Forschung und Statistik (Nr. R [83] 10)	83
6. Deutsche Arbeitsgemeinschaft für Epidemiologie (DAE)	84

Vorwort

Die grundsätzliche Überarbeitung der 1994 vom Berliner Datenschutzbeauftragten herausgegebenen gleichnamigen Broschüre wurde insbesondere deshalb als notwendig angesehen, weil

- zu prüfen war, inwieweit die rechtlichen Vorgaben der EG-Datenschutzrichtlinie neue datenschutzrechtliche Anforderungen an die wissenschaftliche Forschung mit personenbezogenen Daten stellen,
- in den Jahren 1998 und 1999 eine intensive Diskussion zwischen Vertretern des Datenschutzes und der epidemiologischen Forschung sowie zwischen Vertretern der amtlichen Statistik, der Datenschutzbehörden und Forschern der empirischen Wirtschaftsforschung, auch unter dem Aspekt der Sicherung des Forschungsstandortes Deutschland, zwang, nationale und internationale Erfahrungen und Problemstellungen aufzugreifen,
- zwischenzeitlich – z. B. mit dem Einsatz von Treuhändern – neue Erfahrungen gesammelt werden konnten und diese Erkenntnisse zugänglich gemacht werden sollten,
- medizinische Forschungsprojekte – beispielsweise die medizinischen Netzwerke (MEDNET) – zunehmend bundesweit vernetzt sind und sich in Richtung wissenschaftlich multivalent nutzbarer Register entwickeln,
- Lösungsansätze auch für spezielle Fragestellungen gefunden werden konnten.

Rita Wellbrock

Rainer Metschke

1. Verfassungsrechtliche Aspekte

1.1 Regelungen für Konflikte zwischen Forschung und Recht auf informationelle Selbstbestimmung

„Kunst und Wissenschaft, Forschung und Lehre sind frei“ (Art. 5 Abs. 3 Satz 1 Grundgesetz [GG]). Im Grundrechtskatalog des Grundgesetzes ist die Wissenschafts- und Forschungsfreiheit ohne Gesetzesvorbehalt gewährleistet. Eine Reihe von Wissenschaftsgebieten haben den Menschen zum Forschungsgegenstand. Er wird Objekt der Forschung. Die auf diesen Gebieten tätigen Wissenschaftler benötigen in vielen Fällen – zumindest vorübergehend – detaillierte sehr sensible Daten über einzelne Personen. Damit kann die in Art. 5 GG gewährleistete Freiheit von Wissenschaft und Forschung mit dem in Art. 2 i. V. m. Art. 1 GG gewährleisteten allgemeinen Persönlichkeitsrecht in Konflikt geraten. Das allgemeine Persönlichkeitsrecht gewährleistet nach der Rechtsprechung des Bundesverfassungsgerichts auch die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen – das sog. Recht auf informationelle Selbstbestimmung (BVerfGE 65, S. 41 f., s. Anlage 3.1.2). Einschränkungen dieses Rechts sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsmäßigen normklaren gesetzlichen Grundlage und müssen den Grundsatz der Verhältnismäßigkeit wahren.

Können Grundrechte miteinander in Konflikt geraten und ist dies eine allgemeine, nicht nur im Einzelfall auftretende Konstellation, so ist in erster Linie der Gesetzgeber gefordert, Regelungen zu treffen. Diese Regelungen müssen nach der Rechtsprechung des Bundesverfassungsgerichts dem Grundsatz der „praktischen Konkordanz“ entsprechen, d.h., es muss ein Ausgleich zwischen den widerstreitenden Positionen gefunden werden, der es ermöglicht, dass beide Grundrechte möglichst weitgehend realisiert werden können. Der Gesetzgeber muss die rechtlichen Rahmenbedingungen festlegen, unter denen personenbezogene Daten zu Forschungszwecken auf der Grundlage einer Einwilligung der Betroffenen und ohne Einwilligung der Betroffenen verwendet werden dürfen.

Der Gesetzgeber hat diese Regelungen geschaffen. Er hat allgemeine Regelungen zu den inhaltlichen und formalen Anforderungen an rechtswirksame Einwilligungen in die Verarbeitung personenbezogener Daten getroffen (s. 4.) und hat sowohl in den Landesdatenschutzgesetzen und im Bundesdatenschutzgesetz wie auch in zahlreichen spezialgesetzlichen Bestimmungen wie z. B. Landeskrankenhausgesetzen, Meldegesetzen, im Sozialgesetzbuch X, in den Krebsregistergesetzen, Archivgesetzen, im Stasi-Unterlagen-Gesetz die Voraussetzungen festgelegt, unter denen personenbezogene Daten für Forschungszwecke ohne Einwilligung der Betroffenen verarbeitet werden dürfen (s. 5. sowie Anlagen 3 und 4).

Einige Forschungsregelungen haben als Ausgangspunkt eine spezifische Art der Daten (Sozialdaten – Sozialgesetzbuch, Meldedaten – Meldegesetze, archivierte Verwaltungsdaten – Archivgesetze). Andere Regelungen sind auf bestimmte Daten besitzende öffentliche Stellen ausgerichtet (Statistische Ämter – Statistikgesetze, „Gauck-Behörde“ – Stasi-Unterlagen-Gesetz). Diese Spezialregelungen nehmen an Bedeutung zu, da die einzelnen

Wissenschaftszweige (z.B. medizinische und psychologische Forschung, Sozialforschung, zeitgeschichtliche Forschung) aufgrund ihrer verschiedenen Methoden und Informationsinteressen auf ganz unterschiedliche Weise die informationelle Selbstbestimmung der Betroffenen berühren.

Für viele wissenschaftliche Forschungsvorhaben sind nach wie vor die allgemeinen Forschungsregelungen in den Landesdatenschutzgesetzen und im Bundesdatenschutzgesetz einschlägig. Ist die forschende oder den Forschern Daten übermittelnde Einrichtung (Daten besitzende Stelle) eine öffentliche Stelle des Bundes oder eine nicht-öffentliche (private) Stelle, so sind die Regelungen des Bundesdatenschutzgesetzes einschlägig, wenn keine spezielle gesetzliche Grundlage vorhanden ist.

Ist die forschende oder die Daten besitzende Stelle eine öffentliche Stelle des Landes Berlin bzw. des Landes Hessen, so gilt dagegen – falls keine spezielle gesetzliche Forschungsregelung geschaffen wurde – das Berliner Datenschutzgesetz bzw. das Hessische Datenschutzgesetz.

Nicht selten kommt es zu einem Ineinandergreifen von öffentlichen und privaten Einrichtungen, so dass Regelungen unterschiedlicher Rigidität für die Beteiligten eines wissenschaftlichen Vorhabens gelten.

1.2 Eingriffe in das informationelle Selbstbestimmungsrecht – Prüfung des legitimierenden Gemeinschaftsinteresses, des Geeignetheitsgrundsatzes, des Erforderlichkeitsgrundsatzes und des Übermaßverbotes

Unter Zugrundelegung der Rechtsprechung des Bundesverfassungsgerichts und der vom Gesetzgeber getroffenen Regelungen ist bei Forschungsvorhaben, die personenbezogener Daten bedürfen, für jeden Schritt der Verarbeitung dieser Daten, insbesondere durch den Forscher selbst, zu prüfen, ob das Forschungsvorhaben einem legitimen Gemeinschaftsinteresse dient, ob die Verarbeitung zur Erreichung des Forschungszwecks geeignet und notwendig ist und die Eingriffstiefe nicht außer Verhältnis zu dem angestrebtem Zweck steht. Im vorliegenden Zusammenhang bedeutet dies insbesondere, dass jeweils der geringste Eingriff, das mildeste Mittel zur Erreichung des Forschungszwecks gewählt werden muss. Der Betroffene muss keine Eingriffe dulden, die sich – ohne den angestrebten Zweck des Forschungsvorhabens zu gefährden – vermeiden lassen oder auch durch weniger in die Rechte des Betroffenen eingreifende Mittel ersetzt werden können.

Die Übermittlung und Verwendung personenbezogener Daten zu Forschungszwecken hat sich also auf das zum Erreichen des angegebenen Zwecks erforderliche Minimum (Datensparsamkeitsgebot) zu beschränken. Der Forscher muss vor Beginn seiner Datenerhebungen prüfen, ob das Ziel nicht mit einem gleich geeigneten, aber für den Betroffenen weniger belastenden Vorgehen erreicht werden kann. Ergibt sich bei dieser Prüfung von Alternativen, dass der wissenschaftliche Zweck auch mit einem geringer belastenden Verfahren erreicht werden kann, dann ist der Eingriff in der zunächst vorgesehenen Form und Tiefe unverhältnismäßig und verfassungswidrig.

1.2.1 Legitimierendes Gemeinschaftsinteresse

Das für alle Grundrechtseingriffe notwendige legitimierende Gemeinschaftsinteresse wird durch die in Art. 5 Abs. 3 GG enthaltene Gewährleistung der Forschungsfreiheit begründet. Eine Zensur, ob ein Forschungsansatz wertvollen oder minder bedeutsamen Zielen dient,

darf grundsätzlich nicht stattfinden. Die Auswahl der Forschungsthemen gehört zur Grundrechtsgarantie des Art. 5 Abs. 3 GG. Im Bereich von Grundrechtskollision kann jedoch untersucht werden, ob der verfolgte Forschungsansatz auf rechtliche Hindernisse stoßen würde. So sind beispielsweise Forschungen, die die Produktion von ABC-Waffen vorbereiten, wegen Verstoßes gegen die völkerrechtlichen Vereinbarungen der Bundesrepublik Deutschland unzulässig, desgleichen Forschungen, die gegen das Embryonenschutzgesetz verstoßen, oder Forschungen, die mit der ungenehmigten Freisetzung gentechnisch veränderter Bakterien, Viren, anderer Lebewesen oder Pflanzen verbunden sind. Die Erhebung und weitere Verwendung von personenbezogenen Daten für derartige Zwecke ist von vornherein unzulässig, so dass es keiner weiteren Abwägung gegenüber dem Recht auf informationelle Selbstbestimmung bedarf.

1.2.2 Geeignetheitsgrundsatz

Im Rahmen der Geeignetheitsprüfung ist zu untersuchen, ob die zu erhebenden, beizuziehenden oder zu verarbeitenden Daten überhaupt tauglich sind, den angestrebten Untersuchungszweck zu fördern. Steht aufgrund der im Forschungsdesign enthaltenen Hypothesen fest, dass die zu verwendenden Daten nicht geeignet sind, die erforderlichen Nachweise für die aufgestellten Hypothesen zu erbringen, oder ist zu erkennen, dass die Daten nur auf Vorrat gesammelt werden sollen, um später zu definierenden Forschungsvorhaben zu dienen, so liegt kein taugliches Mittel für die Wahrnehmung der grundrechtlichen Freiheit aus Art. 5 Abs. 3 GG vor. Die Erreichung der vorgestellten Forschungsziele ist unmöglich, so dass Datenschutz vorzugehen hat. Die Entscheidung über eine datenschutzrechtlich begründete Zugriffsverweigerung muss auf die unterbreiteten Hypothesen, Forschungsziele und Methoden detailliert eingehen.

1.2.3 Erforderlichkeitsgrundsatz

Erforderlich ist ein eingreifendes Vorgehen ohne oder gegen den Willen des Betroffenen nur, wenn dessen Einwilligung nicht eingeholt werden kann. Grundsätzlich ist das Einholen einer Einwilligung des Betroffenen das vorrangig zu wählende grundrechtskonforme Verfahren zur Erreichung des Forschungszwecks, denn es lässt dem Betroffenen die Möglichkeit, über die Verwendung seiner Daten selbst zu entscheiden, und ist eine für den Betroffenen transparente Verfahrensweise (s. 4.). Liegen die personenbezogenen Daten, die für ein Forschungsvorhaben benötigt werden, bereits einer Stelle vor, so können die Betroffenen in vielen Fällen angeschrieben und um Einwilligung gebeten werden, ohne dass ihre Daten zuvor ohne ihre Kenntnis und ohne ihre Zustimmung an den Forscher übermittelt werden (sog. Adressmittlungsverfahren, s. 6.1). Die Einholung einer Einwilligung ist aber nicht immer ein möglicher Weg, um den Forschungszweck zu erreichen, z. B. dann nicht, wenn es praktisch kaum möglich ist, die aktuellen Adressen der Betroffenen zu ermitteln.

Wenn ein Forschungsvorhaben ohne Einwilligung des Betroffenen durchgeführt werden soll, so verlangt der Erforderlichkeitsgrundsatz die Untersuchung, ob das Forschungsvorhaben unter den geeigneten Mitteln das mildeste Mittel verwenden will, um die angestrebten Zwecke zu erreichen, und ob weniger belastende Alternativen verfügbar sind. Dem Verfassungsgrundsatz entsprechende Formulierungen sind in den meisten datenschutzrechtlichen Vorschriften zu finden. Die Frage, ob unter mehreren Mitteln dasjenige ausgewählt worden ist, das die geringste Beeinträchtigung der informationellen Selbstbestimmung verursacht, betrifft zum einen die zu verarbeitende Datenmenge (Grundsatz der Datensparsamkeit), zum

zweiten die Art der zu verarbeitenden Daten (personenbezogene Daten, anonymisierte oder pseudonymisierte Daten) und zum dritten den Kreis der Personen, die Kenntnis der personenbezogenen Daten erhalten.

Der Erforderlichkeitsgrundsatz gebietet, dass das geplante Forschungsvorhaben eine nachvollziehbare Darlegung erhält, aus der sich die Erforderlichkeit der Verarbeitung erschließen lässt. Insbesondere ist darzustellen, warum das Verfahren nicht mit anonymisierten oder pseudonymisierten Daten abgewickelt werden kann und aus welchen Gründen Verschlüsselungsverfahren und personenbezogene Daten nicht an dritter Stelle (Treuhandverfahren) verwahrt werden können. Der Erforderlichkeitsgrundsatz verlangt von der Wissenschaft, das verfügbare „Methodenarsenal“ auf datenschutzrechtlich besser abgesicherte Verfahren zu überprüfen. Das Forschungsdesign muss erkennen lassen, dass die Frage der verfügbaren Alternativen gestellt und im Sinne des mildesten Eingriffs beantwortet worden ist. Da nur ausnahmsweise ein Methodenmonismus bestehen wird, zwingt der Erforderlichkeitsgrundsatz zu einer vorausgehenden Analyse der Forschungsmethodik. In Anbetracht der erforderlichen Grundrechtseingriffe bei datenschutzrechtlich Betroffenen muss eine solche Vorabanalyse als Voraussetzung der datenschutzrechtlichen Entscheidung über die Freigabe von Daten in jedem Fall gefordert werden. Diese Analyse muss die im Folgenden näher erörterte Prüfung einschließen, ob höhere Datensicherheit durch Trennung der personenbezogenen Daten von anonymisierten oder pseudonymisierten Daten und gesonderte Verwahrung der Verschlüsselungsverfahren erreicht werden kann. Bei zumutbarem Aufwand muss dieser Weg gegangen werden.

1.2.4 Übermaßverbot

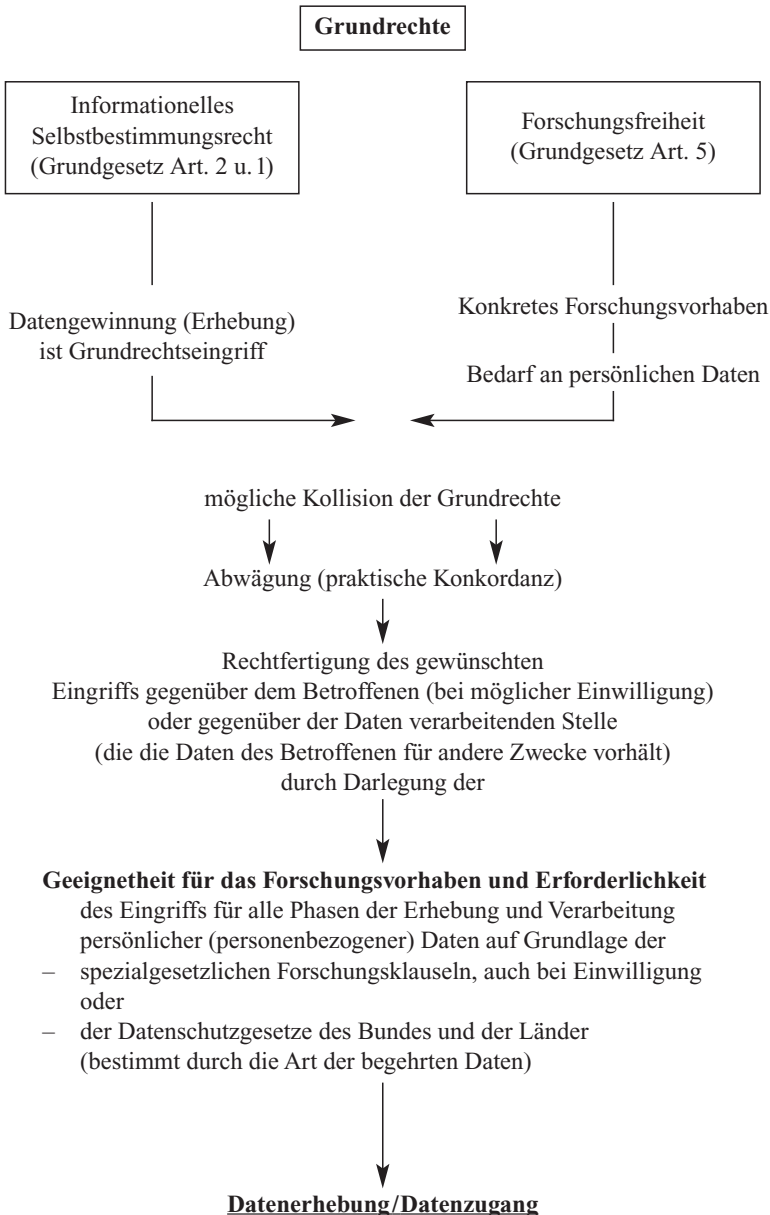
Das verfassungsrechtliche Übermaßverbot verlangt eine Abwägung, ob die mit der ausgewählten und erforderlichen Datenverarbeitung verbundenen Beeinträchtigungen der Betroffenen nicht übermäßig belastend wirken und insofern in einem unangemessenen Verhältnis zum angestrebten Untersuchungszweck stehen. Besonders sensitive Daten – zu ihnen gehören auch Gesundheitsdaten – erfordern eine ausführlichere Begründung des Forschers und besondere Vorkehrungen zur Datensicherheit. Das Übermaßverbot steigert insofern die Anforderungen, die sich bereits aus dem Erforderlichkeitsgrundsatz ergeben.

Im Rahmen des Übermaßverbotes ist auch die Frage zu behandeln, ob Daten aufgrund gesetzlicher Forschungsklauseln gegen den erklärten Willen der Betroffenen zur Verarbeitung in der Forschung freigegeben werden können. Regelmäßig wird das zu verneinen sein, so dass nach erklärtem Widerspruch gegen die Datenverarbeitung nur mit anonymisierten oder pseudonymisierten Daten geforscht werden darf, wenn nicht der gesamte Datensatz zu löschen ist.

Die Übermaßfrage steuert schließlich auch die Möglichkeit zur Veröffentlichung und zu sonstiger Weitergabe von Daten. So hat ein Straftäter das Recht, die Stufe der Resozialisierung erreichen zu können, und kann deswegen sogar der erneuten Verwendung öffentlich zugänglicher Daten in öffentlichen Medien widersprechen (BVerfGE 35, 202, 232, sog. Lebach-Urteil).

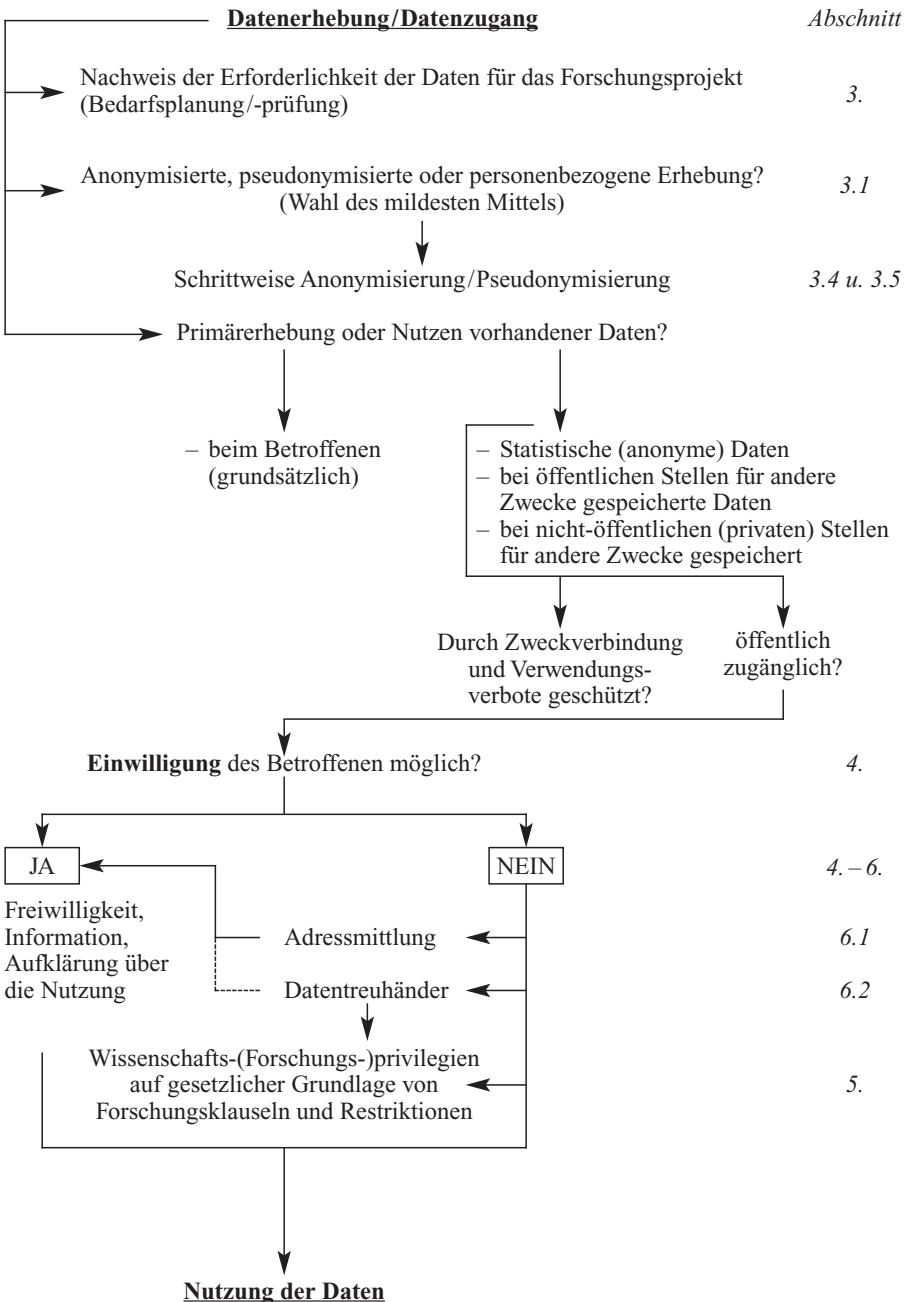
Für die Errichtung von Forschungsregistern, in denen dauerhaft für eine noch nicht absehbare Zahl von Forschungsprojekten personenbezogene Daten verarbeitet werden sollen, besteht gesonderter Regelungsbedarf (s. 8.).

1.3 Übersichtsdarstellung

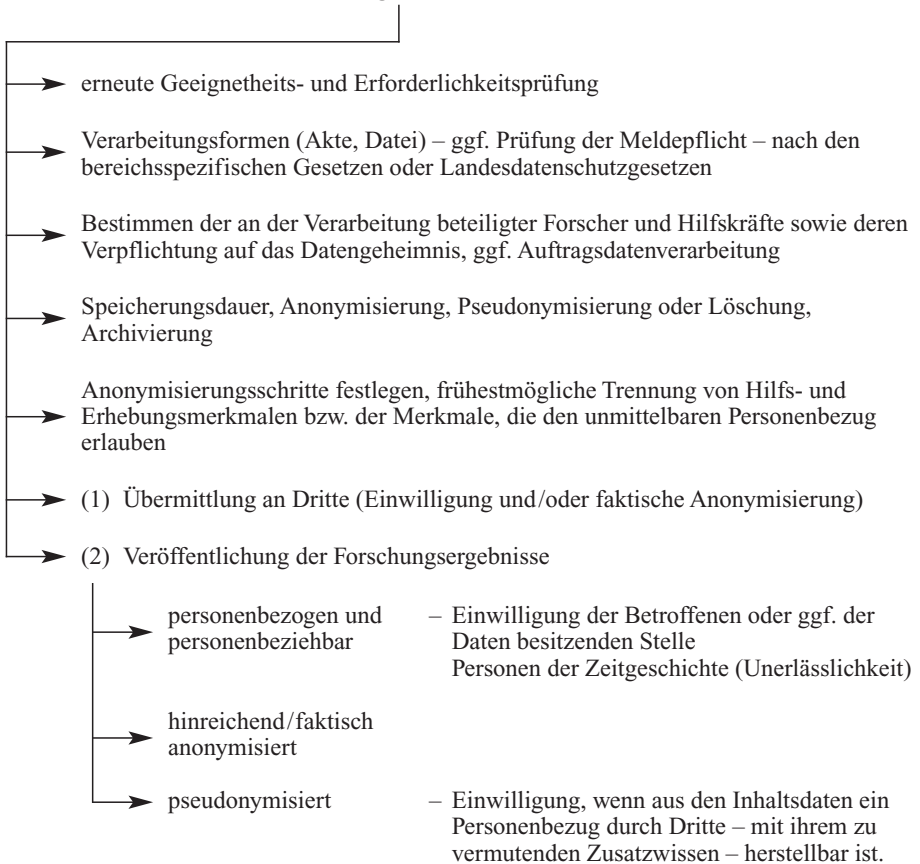


Abschnitt

I.



Nutzung der Daten



2. Rechtliche Vorgaben der EG-Datenschutzrichtlinie – von den Mitgliedsstaaten festzulegende Garantien –

Am 24. Oktober 1994 wurde die EG-Datenschutzrichtlinie („Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“) durch die Europäische Kommission verabschiedet. Sie folgt dem Europaratsübereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten von 1981 als weiterer wichtiger Schritt auf dem Weg zu internationaler Harmonisierung und Verbindlichkeit des Datenschutzrechts. Für die Mitgliedsstaaten der Europäischen Union legt die Richtlinie erstmals einen rechtsverbindlichen grenzüberschreitenden Rahmen fest, in dem personenbezogene Daten nach weitgehend einheitlichen Regelungen verarbeitet werden müssen. Die EG-Datenschutzrichtlinie ist eine Querschnittsregelung, die durch bereichsspezifische Gemeinschaftsvorschriften ergänzt werden kann und soll. Sie fordert von den Mitgliedsstaaten ein Tätigwerden, belässt ihnen aber in der konkreten Ausgestaltung der nationalen rechtlichen Regelungen Spielräume.

Zur Verarbeitung personenbezogener Daten für Forschungszwecke enthält die EG-Richtlinie (EG-RL) einige konkrete Regelungen. In diesen Regelungen werden die Mitgliedstaaten verpflichtet, „geeignete“ bzw. „angemessene“ Garantien festzulegen, damit die mit der Verarbeitung der personenbezogenen Daten verbundenen Eingriffe für die Betroffenen zumutbar sind.

2.1 Zweckdurchbrechung für Zwecke der Forschung

Gemäß Art. 6 Abs. 1b EG-RL (Durchbrechung der ursprünglichen Zweckbindung im Interesse der Forschung) haben die Mitgliedstaaten vorzusehen, dass personenbezogene Daten nur für festgelegte und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken ist im Allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, sofern die Mitgliedsstaaten geeignete Garantien schaffen.

Geeignete Garantien in diesem Sinne sind gesetzliche Regelungen, die die Voraussetzungen für eine Zweckänderung klar und angemessen festlegen. Der Gesetzgeber hat nach der EG-RL Spielräume, wie er die geeigneten Garantien ausgestaltet. Zu den bereits bestehenden rechtlichen Vorgaben an die Forscher – u. a. Zweckbindung der Daten, getrennte Speicherung der Hilfsmerkmale, frühzeitige Anonymisierung bzw. Löschung/Vernichtung der Daten (s. 4. und 5.) –, könnte ein gesetzlich anerkanntes Forschungsgeheimnis eingeführt werden. Es lässt den beim Forscher vorhandenen personenbezogenen Daten einen besonderen Schutz zukommen, indem es verbietet, dass Forscher die Daten an Dritte weitergeben oder dass Dritte (z.B. Strafverfolgungsbehörden) auf die Daten zugreifen. Eine dahingehende Regelung im Strafgesetzbuch und in der Strafprozessordnung mit korrespondierendem Zeugnisverweigerungsrecht der Forscher und Beschlagnahmeverbot für Strafverfolgungsbehörden und Gerichte ist sowohl von Wissenschaftlern als auch von einigen Datenschutzbeauftragten gefordert worden. Sie könnte insbesondere den Schutz der an wissenschaftlichen Studien teilnehmenden Probanden (z.B. bei Dunkelfeldstudien) vor

Strafverfolgung sicherstellen und bei der in den gesetzlichen Forschungsregelungen vorgesehenen Abwägung der Interessen (s. 5.) eine Entscheidung zugunsten der Forscher erleichtern. Die Forderung nach einem zugriffsfesten Forschungsgeheimnis ist jedoch umstritten und die rechtlichen Konsequenzen eines Forschungsgeheimnisses werden kontrovers diskutiert.

2.2 Aufbewahrung für Zwecke der Forschung

Nach Art. 6 Abs. 1e EG-RL (Aufbewahrung personenbezogener Daten für Zwecke der Forschung) dürfen personenbezogene Daten nicht länger aufbewahrt werden, als es für die Realisierung der Zwecke erforderlich ist, für die sie erhoben oder weiterverarbeitet werden, sofern die Identifizierung der betroffenen Person möglich bleibt. Für personenbezogene Daten, die darüber hinaus für historische, statistische oder wissenschaftliche Zwecke aufbewahrt werden sollen, haben die Mitgliedsländer geeignete Garantien festzulegen.

In Deutschland sehen die Regelungen im Bundesarchivgesetz und den Landesarchivgesetzen eine Reihe rechtlicher Vorgaben zur Verarbeitung personenbezogener Daten für Forschungszwecke vor, die als geeignete Garantien in diesem Sinne qualifiziert werden können (s. Anlage 4).

2.3 Information der Betroffenen

Art. 11 Abs. 2 EG-RL (Information der Betroffenen bei Verarbeitungen für Zwecke der wissenschaftlichen Forschung) gibt vor, dass bei Verarbeitungen für Zwecke der Statistik oder der historischen oder wissenschaftlichen Forschung die in Art. 11 Abs. 1 EG-RL festgelegte Verpflichtung zur Information der Betroffenen keine Anwendung findet, wenn die Information der betroffenen Person unmöglich ist, unverhältnismäßigen Aufwand erfordert oder die Speicherung oder Weitergabe durch Gesetz ausdrücklich vorgesehen ist. Auch diese Erleichterung für die Forschung ist durch geeignete Datenschutzgarantien zu sichern.

2.4 Rechtliche Vorgaben für die Verarbeitung sensibler Daten

Gemäß Art. 8 EG-RL (Verarbeitung besonderer Kategorien personenbezogener Daten) sind sensitive Daten insbesondere Daten über rassische oder ethnische Herkunft, politische Meinung, religiöse Überzeugung, Gesundheit oder Sexualleben. Für diese Daten besteht ein grundsätzliches Verbot der Verarbeitung. Nur unter den dort festgelegten engen Voraussetzungen sind Ausnahmen zulässig. Für den Bereich der Forschung gelten insbesondere als Ausnahmen:

- wenn der Betroffene eingewilligt hat,
- wenn die Mitgliedsstaaten aus Gründen eines wichtigen öffentlichen Interesses in einer nationalen Rechtsvorschrift eine Ausnahme vorgesehen haben,
- wenn die Verarbeitung von Daten, die Straftaten, straffrechtliche Verurteilungen oder Sicherungsmaßnahmen betreffen, unter behördlicher Aufsicht erfolgt oder wenn das einzelstaatliche Recht angemessene andere Garantien vorsieht.

Die gesetzlichen Forschungsregelungen in Deutschland können, soweit sie auf die genannten Datenarten Anwendung finden, als nationale Rechtsvorschrift in diesem Sinne qualifiziert werden.

2.5 Sonstige Regelungen

Im Übrigen sind für die Fragen des Verhältnisses von Forschung und Datenschutz in der EG-Datenschutzrichtlinie insbesondere die allgemeinen Regelungen zur Verarbeitung von personenbezogenen Daten auf der Grundlage von Einwilligungen (Art. 7a, s. auch unten 4.) und zur Information der Betroffenen, über die personenbezogene Daten erhoben werden (Art. 10, s. auch unten 4.), von Bedeutung, ferner auch die Ausarbeitung von Verhaltensregeln durch Berufsverbände und andere Vereinigungen (Art. 27). Verhaltensregeln in diesem Sinne können keine gesetzlichen Regelungen ersetzen, sie können jedoch innerhalb des vom Gesetzgeber festzulegenden Rahmens einen angemessenen Ausgleich der kollidierenden Interessen fördern. Sie können ein höheres Schutzinteresse erzeugen, als es der gesetzliche Mindeststandard verlangt.

3. Personenbezogene, anonymisierte und pseudonymisierte Daten

Der Erforderlichkeitsgrundsatz gebietet, dass das geplante Forschungsvorhaben eine nachvollziehbare Darlegung enthält, aus der sich die Erforderlichkeit der geplanten Verarbeitung erschließen lässt. Insbesondere ist darzulegen, warum das Forschungsvorhaben nicht mit anonymisierten oder pseudonymisierten Daten durchgeführt werden kann. Grundsätzlich sollte die Verarbeitung von Daten zu wissenschaftlichen Zwecken in anonymisierter Form erfolgen. Die Probleme des Datenzugangs für die Forschung beziehen sich vorrangig auf Individual- oder Einzeldaten. Nicht selten kann der Datenbedarf jedoch mit anonymisierten Daten abgedeckt werden. Forschung mit sicher anonymisierten Daten ist jederzeit ohne datenschutzrechtliche Vorgaben möglich. Stehen einer Anonymisierung der Daten wissenschaftliche Gründe entgegen, dürfen die Daten in pseudonymisierter Form verarbeitet werden. Erst wenn sowohl einer Anonymisierung als auch einer Pseudonymisierung der Daten wissenschaftliche Gründe entgegenstehen, dürfen auch personenbezogene Daten verarbeitet werden (s. 1.2.3). Ob es sich im Einzelfall um anonymisierte, pseudonymisierte oder personenbezogene Daten handelt, bedarf sorgfältiger datenschutzrechtlicher Prüfung.

Die datenschutzrechtlichen Bestimmungen finden nur Anwendung, wenn für ein Forschungsprojekt personenbezogene Daten benötigt werden.

3.1 Wann sind Daten personenbezogen?

Der Schutzbereich des Rechts auf informationelle Selbstbestimmung umfasst das Recht des Einzelnen, „über die Preisgabe und Verwendung seiner persönlichen Daten“ selbst zu bestimmen (BVerfGE 65, 1 [43]).

Persönliche Daten werden im Datenschutzrecht als „personenbezogene Daten“ bezeichnet und definiert. Personenbezogene Daten sind nach der Legaldefinition des § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbar natürlichen Person (Betroffener). Darauf nimmt auch das Bundesverfassungsgericht in seiner Entscheidung zum Volkszählungsgesetz bei der Beschreibung des Grundrechts auf informationelle Selbstbestimmung Bezug. Es differenziert zwischen einem bestehenden und einem herstellbaren Personenbezug und umschreibt in weiteren Entscheidungen den Schutzbereich des informationellen Selbstbestimmungsrechts mit den auf die Grundrechtsträger „bezogenen individualisierten oder individualisierbaren Daten“ (BVerfGE 67, 100 [144]). Bei Betrachtung dieser Begriffsbestimmung umfasst der Schutzbereich der informationellen Selbstbestimmung nicht nur die Daten einer bestimmten (individualisierten) Person, sondern auch jene Einzelangaben, die eine bestimmte Person zwar nicht eindeutig oder unmittelbar identifizieren, die es aber erlauben, die Identität der Person mit Hilfe anderer Informationen festzustellen. Man bezeichnet diese als individualisierbare bzw. personenbeziehbare Daten.

3.2 Daten Verstorbener

Grundsätzlich wird der Schutzbereich dann relativiert, wenn schutzwürdige Belange des Betroffenen durch seinen Tod nicht mehr berührt werden können. Das Datenschutzrecht

Berlins bezieht in die Definition des Begriffs der personenbezogenen Daten auch die Daten von Verstorbenen mit ein. In den Gesetzen anderer Bundesländer, einschließlich des Hessischen Datenschutzgesetzes, wie auch im BDSG ist dies nicht explizit der Fall.

Zunächst ist festzustellen, dass die Eigenschaft einer Person, Träger eines Grundrechts zu sein, spätestens mit der Geburt beginnt und mit dem Tod endet. Das informationelle Selbstbestimmungsrecht kann also auch nur von lebenden Personen ausgeübt werden. Das heißt aber auch, dass ein Lebender in informationeller Selbstbestimmung Entscheidungen treffen kann, die über seinen Tod hinausreichen und nach Art. 1 Abs. 1 und 3 GG die staatliche Gewalt binden. Darüber hinaus hat das Bundesverfassungsgericht im sog. „Mephisto-Urteil“ (BVerfGE 30, 173 [194]) festgestellt:

„Es würde mit dem verfassungsverbürgten Gebot der Unverletzlichkeit der Menschenwürde, das allen Grundrechten zu Grunde liegt, unvereinbar sein, wenn der Mensch, dem Würde kraft seines Personseins zukommt, in diesem allgemeinen Achtungsanspruch auch nach einem Tode herabgewürdigt oder erniedrigt werden dürfte. Dementsprechend endet die in Art. 1 Abs. 1 GG aller staatlichen Gewalt auferlegte Verpflichtung, dem Einzelnen Schutz gegen Angriffe auf seine Menschenwürde zu gewähren, nicht mit dem Tode.“

In diesem Urteil geht es auch um den Schutz der Angehörigen oder Personen, die dem Verstorbenen nahe verbunden waren. Das Bundesverfassungsgericht stellt hier fest, dass das Schutzbedürfnis und die Schutzverpflichtung in dem Maße schwinden, in dem die Erinnerung an den Verstorbenen verblasst.

Dieser Grundsatz findet sich in verschiedenen Regelungen zu Archivdaten wieder. Hier wurden Sperrfristen aufgenommen, die sich daran orientieren, dass nach Ablauf bestimmter längerer Fristen schutzwürdige Belange nicht mehr berührt werden können. Dabei wurde an Regelungen über Verschollene angeknüpft (BGHZ 50, 133).

3.3 Anonymisierte Daten

Die grundrechtlich geschützte Entscheidungsbefugnis des Einzelnen über seine Daten endet dort, wo verarbeitete Daten keinen Zusammenhang mehr mit seiner Person erkennen lassen.

Werden zunächst personenbezogene Informationen so verändert, dass eine direkte oder indirekte Identifizierung der einzelnen Merkmalsträger unmöglich ist, so werden diese Informationen als (absolut) anonymisierte Daten bezeichnet. Datenschutzrechtliche Nutzungsbeschränkungen bestehen dann nicht mehr. Die Erzeugung anonymisierter Daten aus personenbezogenen Einzelangaben unterliegt aber noch den Datenschutzvorschriften. Die anonymisierende Stelle muss also durch die Einwilligung des Betroffenen oder durch eine Rechtsvorschrift befugt sein, die zunächst personenbezogenen Informationen zu verarbeiten. Ergebnis dieser Verarbeitung sind anonymisierte Einzelangaben, die keinen Hinweis auf eine natürliche Person enthalten oder im Verbund mit anderen Daten erlauben. Nicht anonymisiert sind also alle Einzelangaben einer Person, deren Identität auf Grundlage dieser Daten bestimmt oder bestimmbar ist (personenbezogene Daten).

In der Praxis bereitet die Abgrenzung zwischen den Daten einer bestimmbar Person und anonymisierten Daten gewisse Schwierigkeiten. Bestimmbar ist eine Person, wenn sie mit Hilfe anderer aktuell oder potenziell verfügbarer Informationen, z.B. Aktenzeichen, Geschäftsnummer, detaillierten Informationen über die konkreten Lebensumstände, identifiziert werden kann. Im Regelfall ist eine Person z.B. dann bestimmbar, wenn in einem

umfangreicheren Datensatz lediglich der Name weggelassen wurde, häufig auch dann, wenn Name, Adresse und Geburtsdatum weggelassen wurden. Grundsätzlich hängt die Möglichkeit der Identifizierung einer Person aus einem Datensatz von einer Reihe von Faktoren ab, insbesondere von

- dem möglichen Zusatzwissen (aus allgemein zugänglichen oder nicht allgemein zugänglichen Quellen), das der Daten besitzenden Stelle bzw. einem potenziellen „Angreifer“ zur Verfügung steht,
- den zur Verfügung stehenden technischen Möglichkeiten der Datenverarbeitung,
- der zur Verfügung stehenden Zeit,
- den zur Verfügung stehenden finanziellen Mitteln.

Die Möglichkeiten, von Datensätzen auf Einzelpersonen zu schließen, sind zahlreich. Differenziertes Zusatzwissen über bestimmte Personengruppen, Merkmalskombinationen oder eine Einsicht in öffentlich zugängliche Melderegister, Telefon-CD-ROMs, Adressbücher, Wählerverzeichnisse etc. kann zur Bestimmbarkeit einer Einzelperson führen. Nach dem Stand der Technik können vielfach sogar aus aggregierten Datensätzen individuelle Datensätze reproduziert werden. Aufgrund des ständig weiterentwickelten Standes der Technik gibt es in der Praxis äußerst selten absolut anonymisierte Daten, d. h. Daten, die unter keinen denkbaren Umständen – z. B. unter Verwendung mathematisch-statistischer Verfahren – deanonymisiert werden könnten.

Trotz aller Anonymisierungsbemühungen bleibt also – sollen die Daten für die beabsichtigte Forschung noch verwertbar sein – ein Restrisiko der Deanonymisierung.

Ganz überwiegend wird in neuerer Zeit eine realitätsbezogene Abgrenzung der anonymisierten von den personenbezogenen Daten vorgenommen, derzufolge eine relative, „faktische“ Anonymisierung der Daten ausreichend ist. Von faktisch anonymisierten Daten wird gesprochen, wenn eine Person nur mit einem völlig unverhältnismäßigen Aufwand reidentifiziert werden kann.

Im Volkszählungsurteil verweist das Bundesverfassungsgericht im Zusammenhang mit den notwendigen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung auf das Gebot einer möglichst frühzeitigen „(faktischen) Anonymisierung“ der Daten. Das Gericht führt in einem späteren Urteil aus, dass von Verfassungs wegen lediglich eine faktische Anonymität der Daten geboten ist.

Eine entsprechende – am Grundsatz der Verhältnismäßigkeit orientierte – Definition enthält § 3 Abs. 7 BDSG:

„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.“

Eine ähnliche Definition enthält § 16 Abs. 6 BStatG:

„Für die Durchführung wissenschaftlicher Vorhaben dürfen vom Statistischen Bundesamt und den statistischen Ämtern der Länder Einzelangaben an Hochschulen oder sonstige Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung übermittelt werden, wenn die Einzelangaben nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft zugeordnet werden können und die Empfänger Amtsträger, für den öffentlichen Dienst besonders Verpflichtete oder Verpflichtete nach Abs. 7 sind.“

Hinreichend oder faktisch anonymisierte Daten sind personenbeziehbare (individualisierbare) Daten, bei denen das Risiko der Bestimmbarkeit infolge ihres Inhalts und ihres Verwendungskontextes so weit gemindert ist, dass dem Betroffenen das (Rest)Risiko einer Deanonymisierung zugemutet werden kann. Ist das Risiko einer Deanonymisierung im Einzelfall noch zu groß, kann es u. U. durch zusätzliche technische und organisatorische Maßnahmen, u. a. das Trennungs- und Lösungsgebot, das Zweckbindungsgebot, ein strafbewehrtes Reidentifizierungsverbot, ein Weitergabe-(Übermittlungs-)verbot und eine Aufzeichnungspflicht, weiter verringert werden. Bei der Bestimmung des Deanonymisierungspotenzials ist der aktuelle Stand von Wissenschaft und Technik zu berücksichtigen.

Die Grenze zwischen personenbeziehbaren und faktisch anonymisierten Daten ist damit fließend. Sie kann nur im Einzelfall – unter Berücksichtigung des gegenwärtigen und künftigen (z. B. wirtschaftlichen) Wertes der zu erlangenden Information oder der dem Empfänger sowie einem potenziellen Angreifer zur Verfügung stehenden Ressourcen – bestimmt werden. In der Praxis ist dies für die übermittelnde Stelle mit Schwierigkeiten verbunden. So verlangt dies auch eine Prognose über die Ressourcen der Empfänger der Daten oder eine Einschätzung des Werts der Informationen für potenzielle Angreifer. In einigen wenigen Bundesländern wird Anonymisierung im Sinne einer absoluten Anonymisierung verstanden, d. h., durch die Formulierung bzw. Interpretation der landesrechtlichen Regelungen werden Einzelangaben nur dann als anonym qualifiziert, wenn sie unter keinen Umständen mehr zuzuordnen sind.

Es bieten sich verschiedene Möglichkeiten an, durch Verschlüsselungen und Codierungen einen offenen Personenbezug, wie es der Name darstellen würde, zu vermeiden. Zwei Beispiele werden in Anlage 2 angegeben. Dabei sollten Codierungen bevorzugt werden, die der Betroffene selbst vornimmt und die von ihm jederzeit rekonstruierbar sind. So können den Datensätzen der einzelnen Personen weitere Angaben zugeordnet und Doppelungen vermieden werden. Bei großen Registern könnte auch eine maschinelle, auf Zufallsangaben beruhende Verschlüsselung vorgenommen werden.

3.4 Anonymisierungsverfahren

Die gebräuchlichsten Anonymisierungsmethoden sind:

- das formale Anonymisieren der Datensätze,
- das Verallgemeinern und das Mikro-Aggregieren (kleinerer) Datensätze,
- das Einstreuen von Zufallsfehlern,
- das Zerlegen von Datensätzen in separate Merkmalsbereiche,
- das Ziehen von Stichproben und Unterstichproben (Sub-Sampling),
- das Nutzen von Schlüsseln und Codierungen.

Diese Verfahren führen aber häufig nicht im ersten Schritt zu einer faktischen Anonymisierung. Dies wird manchmal erst nach mehreren Schritten oder durch Kombination der Verfahren erreicht.

Einige Forschungsfragen scheinen die Verarbeitung anonymisierter Daten auszuschließen, wenn das Ziel erreicht werden soll. Hier sei insbesondere auf die empirische Sozialforschung und die historische bzw. zeitgeschichtliche Forschung verwiesen. Auch Längsschnittstudien und Forschungsregister verlangen häufig ein eindeutiges und handhabbares Unterscheidungskriterium, um spätere Angaben der richtigen Person zuzuordnen.

Aber auch die auf der Grundlage von Ehrenkodizes bestehende Verpflichtung der Wissenschaftler zur Speicherung und Archivierung der Einzeldaten und zur Gewährleistung der Überprüfbarkeit der Authentizität der verwendeten Daten durch unabhängige Gremien steht einer frühzeitigen Anonymisierung teilweise entgegen (s. hierzu noch unten 7.1).

3.5 Pseudonymisierungsverfahren

Im Gegensatz zur Anonymisierung ist die Pseudonymisierung nur bedingt eine rücknahme-feste Prozedur. Bei der Pseudonymisierung werden die unmittelbar eine Person identifizierenden Daten durch eine für das Einzelvorhaben zu bildende Zuordnungsvorschrift derart verändert, dass das so gebildete Pseudonym nur mit Kenntnis dieser Zuordnungsvorschrift wieder einer natürlichen Person zugeordnet werden kann. So werden die Identifikationsdaten wie Namen und Anschrift, Versichertennummer, Matrikelnummer etc. durch eine im Einzelfall gewählte Zuordnungsvorschrift in ein Pseudonym überführt. Bei zwingender Notwendigkeit und unter Einhaltung vorher festgelegter rechtlicher Voraussetzungen kann aber der Personenbezug von einer hierzu berechtigten Stelle wieder hergestellt werden. Wer unter welchen Voraussetzungen den Personenbezug wiederherstellen darf, ist eine Frage des Einzelfalls. Die Entschlüsselungsbefugnis sollte möglichst bei der Stelle liegen, die über die personenbezogenen Daten ohnehin verfügt, oder bei einer von der forschenden Institution getrennten, rechtlich selbständigen Stelle.

Beim Einsatz von Pseudonymisierungsverfahren ist stets vorher zu klären,

- ob die identifizierenden Daten durch eine nicht sprechende Nummer ersetzt werden können oder ob sie verschlüsselt werden sollen,
- wer über die Zuordnungstabellen bzw. das Verschlüsselungsverfahren verfügen soll,
- wer das Pseudonym generieren soll,
- ob ein Reidentifizierungsrisiko hinsichtlich der pseudonymisierten Datensätze ausgeschlossen werden kann,
- wer und unter welchen rechtlichen Voraussetzungen Pseudonym und Identifikationsdaten zusammenführen darf.

Bei vielen Forschungsprojekten kamen in der Vergangenheit die Wissenschaftler der Verpflichtung zur frühestmöglichen Trennung der die Person identifizierenden Merkmale dadurch nach, dass dem Datensatz eine Nummer gegeben wurde und beim Projektleiter oder einem vertrauenswürdigen Dritten eine Zuordnungsliste von Nummern, Namen und ggf. Anschriften unter Verschluss vorgehalten wurde. Im Unterschied dazu bietet die „betroffene kontrollierte Pseudonymisierung“ die Möglichkeit, dass schon im Moment der Datenerhebung keine Namen oder Ähnliches erfasst werden. Dies ist möglich, wenn der Betroffene die Merkmale des Pseudonyms aufgrund feststehender Angaben selbst generiert, d.h. sich also selbst ein Pseudonym gibt. Die Merkmale, die zur Generierung des Pseudonyms verwendet werden, sind dann nur dem Betroffenen bekannt. Damit ist eine Reidentifizierung grundsätzlich nur durch den Betroffenen selbst möglich.

In das Pseudonymisierungsverfahren können Daten eingehen wie Namensbestandteile (einzelne Buchstaben, Namenslängen), Teile des Geburtsdatums, das Geschlecht, Namensbestandteile des Geburtsortes oder Tag der Generierung. Diese Daten können sich sowohl auf den Betroffenen selbst als auch auf seine Eltern, Geschwister oder Kinder beziehen. Die Vergabe von Fantasienamen als Pseudonym birgt bei Längsschnittstudien oder Wiederholungsbefragungen die Gefahr des Vergessens oder Verwechselns in sich.

Bei der Pseudonymisierung durch eine mathematische Verschlüsselungstechnik ist hingegen keine unmittelbare Kontrolle der Pseudonymisierung durch den Betroffenen möglich. Er ist darauf angewiesen zu glauben, dass beispielsweise durch eine zweifache Verschlüsselung seiner Identifizierungsdaten ein Pseudonym entsteht, das auch bei einer Umkehr der Verschlüsselungsfunktionen nicht wieder zu den unmittelbaren Identifizierungsdaten zurückführt. Dies wird insbesondere dann transparent und glaubhaft, wenn die Stelle, die die Ausgangsdaten verwahrt und die Pseudonyme berechnet, sowohl gegenüber dem Betroffenen als auch gegenüber dem Forschenden ein vertrauenswürdiger unabhängiger Dritter (im Sinne eines Datentreuhänders) ist. Wenn durch die Pseudonymisierung gegenüber der Trennung von Erhebungs- und Hilfsmerkmalen ein qualitativer Sprung in Richtung Anonymisierung erreicht werden soll, darf die forschende oder die Register führende Stelle nicht in der Lage sein, die Pseudonyme selbst zu berechnen. Wenigstens ein Verschlüsselungsalgorithmus muss immer geheim bleiben.

Wenn pseudonymisierte Daten für die Durchführung eines Forschungsvorhabens ausreichen, muss dieser Weg gewählt werden und von einer Übermittlung personenbezogener Daten an den Forscher abgesehen werden (Grundsatz des geringstmöglichen Eingriffs). Sachgerecht ist, dass die Daten besitzende Stelle die Daten vor der Übermittlung an den Forscher pseudonymisiert oder – insbesondere wenn Datenbestände verschiedener Stellen zusammengeführt werden sollen – dass zwischen die Stelle, die die unverschlüsselten Ausgangsdaten hat, und den Forscher, der die Daten später verarbeiten soll, ein Datentreuhänder geschaltet wird, der die personenbezogenen Ausgangsdaten pseudonymisiert und nur in der pseudonymisierten Form an den Forscher weiterleitet (s. hierzu unten 6.2).

Wenn erst beim Forscher selbst die Identifikationsdaten mit einem Pseudonym versehen werden und anschließend die Identifikationsdaten mit den Pseudonymen und der pseudonymisierte Datenbestand getrennt gespeichert werden, handelt es sich lediglich um eine Maßnahme der Datensicherheit beim Forscher. Eine solche Maßnahme ist bei der Verarbeitung personenbezogener Daten auf der Grundlage einer Forschungsregelung (s. 5.) generell vorgeschrieben. Rechtlich ist in diesem Fall davon auszugehen, dass der Forscher personenbezogene Daten verarbeitet, da er jederzeit in der Lage ist, den Personenbezug wiederherzustellen.

Pseudonyme sollten möglichst nicht anwendungsübergreifend eingesetzt werden, weil sonst das Reidentifizierungsrisiko steigt. Besonders gefährlich ist es, jeden Bürger mit einem einheitlichen Pseudonym zu versehen, das in allen rechtlichen Zusammenhängen gilt (Gesundheitssystem, Krankenversicherung, Steuer, Führerschein, Melderegister etc.). Auch gegen die Verwendung eines einheitlichen Pseudonyms im gesamten Forschungsbereich im Sinne eines einheitlichen persönlichen Forschungskennzeichens bestehen verfassungsrechtliche Bedenken.

Die Qualität der Pseudonymisierungsprozedur hängt von den gleichen Einflussfaktoren ab wie die Stärke der Anonymisierungsprozedur. Unter sonst gleichen Bedingungen ist die Anonymisierung dabei immer datenschutzfreundlicher als die Pseudonymisierung.

4. Verarbeitung personenbezogener Daten auf der Grundlage einer Einwilligung der Betroffenen

Die Mehrzahl der Forschungsvorhaben wird nicht mit Hilfe schon vorliegender, anonymisierter oder pseudonymisiert übermittelter Einzeldaten durchgeführt werden können. Wenn für ein Forschungsvorhaben personenbezogene Daten benötigt werden, kommt in erster Linie eine Verarbeitung der Daten auf der Grundlage einer Einwilligung der Betroffenen in Betracht, denn dieses Verfahren lässt den Betroffenen ihre Entscheidungsfreiheit bezüglich der Verarbeitung ihrer Daten und ist für sie transparent (s. oben 1.).

Mit der Erteilung oder Versagung einer Einwilligung wird die „Befugnis des Einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten“ (Volkszählungsurteil des Bundesverfassungsgerichts) zu bestimmen, ausgeübt. Der Einzelne soll nicht zum bloßen Informationsobjekt werden. Dies setzt voraus, dass er auch tatsächlich im Einzelfall die Möglichkeit hat zu entscheiden, ob und unter welchen Bedingungen seine Daten verarbeitet werden. Um dies sicherzustellen, legen die datenschutzrechtlichen Regelungen zur Einwilligung in die Verarbeitung personenbezogener Daten bestimmte inhaltliche und formale Anforderungen an die Einwilligung fest (vgl. z.B. § 6 BlnDSG, § 7 HDSG, § 4 BDSG), insbesondere die konkrete Benennung des vorgesehenen Zwecks der Verwendung der Daten, ausreichende Information des Betroffenen über die vorgesehene Verarbeitung seiner Daten, i. d. R. Schriftlichkeit der Einwilligung, die Freiwilligkeit der Einwilligung und die Möglichkeit des Widerrufs der Einwilligung.

Diese inhaltlichen und formalen Anforderungen an die Einwilligungserklärung sollen sicherstellen, dass eine Verarbeitung personenbezogener Daten auf der Grundlage einer Einwilligung nur erfolgt, wenn der Betroffene klar und eindeutig eingewilligt hat.

Die Regelungen zu den inhaltlichen und formalen Anforderungen an die Einwilligungserklärungen entsprechen auch den Vorgaben der EG-RL. So haben gemäß Art. 7 EG-RL die Mitgliedsstaaten vorzusehen, dass eine Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn eine der in a bis f der Vorschrift geregelten Voraussetzungen erfüllt ist; zu diesen Voraussetzungen zählt, dass der Betroffene seine Einwilligung „ohne jeden Zweifel“ gegeben hat.

4.1 Informierte Einwilligung durch Aufklärung

Entscheidungsfreiheit bedeutet, dass der Betroffene Art und Umfang der Verarbeitung der persönlichen Daten selbst mitbestimmt. Keine Verarbeitung darf beispielsweise unter Ausnutzung einer pauschalen Einwilligung hinter dem Rücken des Betroffenen, ohne oder gegen seinen Willen erfolgen. Damit der Betroffene wirksam in die Verarbeitung seiner Daten einwilligen kann, ist er nicht nur über die Erhebung, sondern auch über jeden weiteren beabsichtigten Verarbeitungszweck konkret zu informieren. So kann er die Folgen seiner Einwilligung absehen.

Eine informierte Einwilligung liegt dann vor, wenn der Betroffene ausdrücklich und unübersehbar über die wesentlichen Modalitäten der vorgesehenen Verarbeitung seiner Daten

aufgeklärt worden ist. Hierzu sind im Regelfall die folgenden Informationen über das Forschungsvorhaben zu zählen:

- verantwortlicher Träger und Leiter des Forschungsvorhabens,
- Zweck des Forschungsvorhabens,
- Art und Weise der Verarbeitung der Daten,
- Personenkreis, der von den personenbezogenen Daten Kenntnis erhält,
- in die Studie einbezogene Kooperationspartner, soweit sie mit eigenständigen Aufgaben bei der Verarbeitung personenbezogener Daten betraut sind,
- Zeitpunkt der Löschung bzw. Vernichtung der personenbezogenen Daten,
- evtl. Empfänger und Abrufberechtigte, denen die Daten verfügbar gemacht werden können.

Zusätzlich ist der Betroffene über sein Recht zu informieren, die Einwilligung in die weitere Verarbeitung seiner Daten zu widerrufen. Darüber hinaus stehen ihm selbstverständlich unabhängig von der Erwähnung in der Einwilligungserklärung

- das Recht auf Auskunft und Einsicht in die seine Person betreffenden Daten und
- das Recht auf Berichtigung fehlerhaft gespeicherter Daten zu.

Gemäß Art. 10 der EG-RL müssen die Mitgliedsstaaten Regelungen treffen, in denen festgelegt ist, welche Informationen bei der Erhebung personenbezogener Daten bei der betroffenen Person (auch bei der Erhebung nach Einwilligung) von dem für die Datenverarbeitung Verantwortlichen mindestens zu geben sind. Konkret aufgeführt sind hier die folgenden Angaben:

- a) Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls eines Vertreters,
- b) Zweckbestimmungen der Verarbeitung, für die die Daten bestimmt sind,
- c) weitere Informationen, beispielsweise betreffend
 - weitere Empfänger oder Kategorien der Empfänger der Daten,
 - die Frage, ob die Beantwortung der Fragen obligatorisch oder freiwillig ist, sowie mögliche Folgen einer unterlassenen Beantwortung,
 - das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten, sofern sie unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

Diese Vorgaben der EG-RL werden durch die dargelegten Regelungen der deutschen Datenschutzgesetze bzw. ihre Interpretationspraxis erfüllt.

Die Informationen, aufgrund derer sich der Betroffene für die Einwilligung in die Verarbeitung seiner Daten entscheidet, sind für den Forscher verbindlich, eine spätere Änderung der Zweckbestimmung der Verarbeitung, der Identität des für das Forschungsvorhaben Verantwortlichen etc. wäre von der Einwilligung zur Verarbeitung personenbezogener Daten nicht mehr gedeckt. Andernfalls wäre der Zweck der datenschutzrechtlichen Regelungen zur Einwilligung, die Entscheidungsfreiheit des Einzelnen zu stärken, in Frage gestellt. In der Praxis kann das allerdings bei der Durchführung des Forschungsvorhabens zu Problemen führen, wenn wissenschaftliche Fragestellungen sich ändern, in die Studie einbezogene Kooperationspartner wechseln etc. Aus wissenschaftlicher Sicht kann es bei einzelnen

Forschungsvorhaben wichtig werden, die Daten für die Bearbeitung neuer oder veränderter Fragestellungen zu nutzen, die zum Zeitpunkt der Einwilligungserklärung des Betroffenen noch nicht bekannt waren und daher in die Angaben zum Zweck der Verwendung der Daten nicht einbezogen werden konnten. Eine erneute Kontaktierung des Betroffenen ist nicht immer möglich oder wäre u. U. mit zusätzlichem hohem Aufwand und Kosten verbunden und könnte wegen Umzug, Tod, Desinteresse etc. der Betroffenen möglicherweise auch zu Problemen im Hinblick auf die Repräsentativität der Daten führen.

Es ist zu beachten, dass die Möglichkeit besteht, Einwilligungserklärungen so zu formulieren, dass eine evtl. inhaltliche Änderung bzw. Ausweitung der Fragestellungen der Studie mit umfasst ist. Grundsätzlich muss eine Einwilligungserklärung hinreichend bestimmt sein. Die Anforderungen an die Vollständigkeit und Präzision der Einwilligungserklärungen können jedoch je nach der konkreten Verarbeitungssituation variieren. Bei der Verarbeitung personenbezogener Daten im Wissenschaftsbereich ist eine weitere Formulierung des Zwecks als in anderen Lebensbereichen vertretbar und nicht unangemessen. Sie entspricht der wissenschaftlichen Arbeitsweise. Es ist eine Entscheidung der Betroffenen, inwieweit sie auch eine Einwilligungserklärung mit einer weiteren Formulierung für die Zwecke der Studie unterschreiben (Frage der Akzeptanz). Auch abgestufte Einwilligungserklärungen haben sich bewährt. So kann zwischen der Einwilligung zu dem unmittelbaren Projekt und der Einwilligung in ein mögliches Nachfolgevorhaben unterschieden werden.

Die Daten besitzende Stelle – z. B. Klinikum, Institut, Forschungsverbund – muss in der Einwilligungserklärung konkret und verbindlich genannt werden. Aus datenschutzrechtlicher Sicht ist es von zentraler Bedeutung, dass die Verantwortlichkeit für die personenbezogenen Daten dauerhaft klar geregelt ist. Ferner muss der Bürger eindeutig darüber informiert worden sein, an wen er sich mit seinen Auskunftersuchen, Widerruf seiner Einwilligung, dem Verlangen nach Datenberichtigung etc. wenden kann. Die Namen der in die Studie einbezogenen Kooperationspartner müssen nur dann konkret aufgeführt werden, wenn sie mit einer eigenständigen Auswertung der personenbezogenen Daten befasst sind. Schließlich sind alle in Aussicht genommenen Institutionen zu benennen, die Zugriff auf die Datenbestände erhalten sollen.

Der vorgesehene Zeitpunkt der Löschung bzw. der Vernichtung der personenbezogenen Daten sollte bereits in der Einwilligungserklärung möglichst konkret benannt werden. Er sollte grundsätzlich daran orientiert sein, wie lange die personenbezogenen Daten für die Durchführung des Forschungsvorhabens benötigt werden. Häufig wird das Problem auftreten, dass für die wissenschaftliche Akzeptanz bzw. Nachprüfbarkeit der Forschungsergebnisse das Vorhandensein der anonymisierten Daten nach der Publikation nicht ausreichend ist. In diesem Fall kann eine Speicherung der personenbezogenen Daten oder der pseudonymisierten Daten für einen bestimmten Zeitraum nach der Publikation der Forschungsergebnisse notwendig sein. Im Falle der Zwischenschaltung eines Datentreuhänders, bspw. eines Notars, dem allein ein Personenbezug möglich ist, stehen einer länger dauernden Speicherung regelmäßig wenig Bedenken entgegen. Diesem Vorgehen sollte daher Vorrang eingeräumt werden (s. 7.1).

4.2 Zweckbindung durch konkrete Benennung des Forschungsvorhabens

Mit Hilfe der „informierten“ Einwilligung beschränkt der Betroffene die Befugnis, seine Daten zu verarbeiten, auf bestimmte Zwecke. Die Zweckbindung ist damit das entscheidende Sicherungsinstrument, das die Einwilligung für den Betroffenen in sich birgt. Der mit

der Einwilligung legitimierte Zweck begrenzt die Möglichkeiten des Datenempfängers, über die Daten des Betroffenen verfügen zu können.

Eine Einwilligung, bei der der Betroffene nicht erkennen kann, zu welchen Forschungsvorhaben seine Daten verwendet werden, ist unwirksam (vgl. z.B. § 6 Abs. 4 BlnDSG, § 7 Abs. 2 HDSG, § 4 Abs. 2 BDSG). Die Einwilligungserklärung muss den konkreten Verwendungszweck – das vorgesehene Forschungsvorhaben – klarstellen. Unzulässig wäre es, auf eine unbegrenzte Anzahl künftiger Forschungsvorhaben oder auf nicht konkretisierte Forschungsvorhaben, über die sich der Betroffene noch keine Vorstellung machen kann, zu verweisen (s. aber auch 4.2 zu nicht voraussehbaren Änderungen bei der Durchführung des Forschungsvorhabens).

4.3 Freiwilligkeit der Einwilligung

Selbstbestimmung setzt „Entscheidungsfreiheit“ über die vorzunehmenden oder zu unterlassenden Handlungen voraus. Da der Schutz der informationellen Selbstbestimmung die Fremdbestimmung ausschließen soll, muss die Einwilligung freiwillig erteilt werden. Eine Einwilligung unter Zwang oder Täuschung widerspricht dem Selbstbestimmungsrecht. Der Betroffene muss, ohne einen Nachteil befürchten zu müssen, die Einwilligung auch verweigern können. Die Selbstbestimmung des Betroffenen ist daher durch entsprechende Vorkehrungen gegen Fremdbestimmung zu sichern. So wäre es mit den datenschutzrechtlichen Regelungen nicht vereinbar, dass ein Krankenhaus die Behandlung des Patienten davon abhängig macht, dass er eine Einwilligungserklärung unterschreibt, der zufolge er seine personenbezogenen Daten umfassend für Forschungszwecke zur Verfügung stellt. Der Betroffene ist nach den datenschutzrechtlichen Regelungen unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass er die Einwilligung verweigern oder sie später widerrufen kann.

In der Praxis zeigt es sich oft, dass die Betroffenen beim Unterschreiben von Einwilligungserklärungen keine tatsächliche Entscheidungsfreiheit haben – z.B. bei staatlichen Leistungen, bei Abschluss von Versicherungsverträgen oder bei Einrichtung eines Bankkontos. Hier müssen die Betroffenen regelmäßig, um das Ziel ihrer Bemühungen nicht zu gefährden, in die Verarbeitung ihrer Daten, häufig sogar in den Abruf weiterer Daten (SCHUFA, Finanzamt etc.), einwilligen. Aus der tatsächlichen Bedrohung der Entscheidungsfreiheit durch die Unterlegenheit des Betroffenen kann aber nicht der Schluss gezogen werden, die „Entscheidungsfreiheit“ des Einzelnen sei zu vernachlässigen, weil sie ohnehin durch die Realität entwertet sei. Aus der unmittelbaren Geltung des Rechts auf informationelle Selbstbestimmung folgt hingegen, dass der grundrechtliche Schutz der Entscheidungsfreiheit nicht durch eine extensive Gestaltung der Einwilligung zur reinen Fiktion werden darf. Die Entscheidungsfreiheit des Einzelnen über eine Einwilligungserklärung muss durch eine sozial adäquate, restriktive Gestaltung der Einwilligungserklärung gesichert werden. Die Autonomie des Betroffenen wird insbesondere sichergestellt durch differenzierte rechtliche Regelungen bzw. Rechtsinterpretationen zur Rechtswirksamkeit und zur Tragweite von Einwilligungen und nicht zuletzt durch den rechtspolitischen Einsatz der Datenschutzbeauftragten für datenschutzgerechtere Verfahren in den Fällen, in denen der einzelne Bürger angemessene Modalitäten des Verfahrens nicht alleine verhandeln bzw. durchsetzen kann.

Die Freiwilligkeit der Entscheidung kann vor allem bei Personen, die auf gerichtliche oder behördliche Anordnung in einer Anstalt untergebracht oder von staatlichen Fürsorgeleitungen abhängig sind, in Frage gestellt sein. Nach dem Arzneimittelgesetz sind klinische

Prüfungen an Probanden, die auf gerichtliche oder behördliche Anordnung in einer Anstalt untergebracht sind, nicht zulässig (§ 40 Abs. 1 Nr. 3 AMG). Hintergrund für diese Regelung ist, dass eine freie Entscheidung in dieser Situation schwierig gewährleistet werden kann, jedenfalls kaum nachprüfbar ist. Außerhalb des Anwendungsbereichs des Arzneimittelgesetzes sollte bei vergleichbaren Konstellationen die Freiwilligkeit der Einwilligung besonders sorgfältig geprüft werden.

4.4 Schriftlichkeit der Einwilligung

Die datenschutzrechtlichen Regelungen verlangen generell die Schriftform bei der Einholung von Einwilligungen. Für die Forschung ergeben sich hieraus mitunter Probleme. So wird darauf verwiesen, dass Telefoninterviews, die im Rahmen der empirischen Sozial-, aber auch der Marktforschung aus Kostengründen eine wachsende Bedeutung gewinnen, unter der Anforderung einer strikten Schriftform wohl kaum durchgeführt werden können, weil der Betroffene vor dem Interview im Regelfall nicht bzw. nur mit großem Aufwand schriftlich um seine Einwilligung gebeten werden kann. Mit der Schriftform wird auch bei anderen Befragungsformen eine erhöhte Verweigerungsrate der Betroffenen in Zusammenhang gebracht. Die Schriftform erwecke Misstrauen vor dem „Kleingedrucktem“. So würden bei höheren Verweigerungsraten bei bestimmten sozialen Gruppen repräsentative Erhebungen erschwert.

Grundsätzlich kann über das Recht auf informationelle Selbstbestimmung schriftlich wie mündlich verfügt werden. Allerdings hat die Schriftform eine – die Ausübung der Selbstbestimmung flankierende und sie schützende – Garantiefunktion. Sie ist eine die Grundrechtsausübung sichernde verfahrensrechtliche Vorkehrung. Sie dient auch Beweis Zwecken, die die Daten besitzende Stelle sichern.

Der Sinn der Schriftform liegt in dem Schutz des Betroffenen vor einer übereilten oder unbedachten Einwilligung. Er soll durch die vorausgehende Information und deren Reflexion dazu veranlasst werden, sich über die Bedeutung seiner Erklärung und Gedanken zu machen. Gleichzeitig wird durch die Schriftlichkeit der Einwilligung die notwendige Transparenz der Datenverarbeitung gesichert. Die mit der Einwilligung bestimmten Grenzen der Verarbeitung können bei Unterzeichnung, aber auch später verlässlich nachvollzogen, hinterfragt und durch den Betroffenen selbst oder die Datenschutzbeauftragten kontrolliert werden. Die Schriftform sichert die Selbstbestimmung auch insofern, als im Streitfall nicht der Betroffene, sondern der Empfänger nachweisen muss, dass eine ausreichende, die Datenverarbeitung legitimierende Einwilligung besteht. Bei schriftlicher Einwilligung sind mögliche Zweifel über die Reichweite der Einwilligung besser vermeidbar als beim „flüchtigen Wort“. Die Regelungen des § 6 Abs. 3 Satz 1 BlnDSG, § 7 Abs. 2 Satz 1 HDSG, § 4 Abs. 2 BDSG gehen deswegen für den Regelfall von der Schriftform aus und gewähren zugleich den notwendigen Spielraum, indem sie die Schriftform der Einwilligung nur gebieten, „soweit nicht wegen besonderer Umstände eine andere Form angemessen ist“ (s. auch die diese Formulierung für den Bereich der Forschung konkretisierende Regelung des § 4 Abs. 3 BDSG). Eine mündliche Einwilligung und die besonderen Umstände, die ein Absehen von der Schriftform im Einzelfall angemessen erscheinen lassen, sollten in jedem Fall durch den Wissenschaftler in geeigneter Form dokumentiert werden.

Dementsprechend kann es bei Telefoninterviews zulässig sein, die schriftliche Einwilligung durch eine ausdrückliche mündliche Einwilligung zu ersetzen und in der Interviewniederschrift zu vermerken. Dies gilt insbesondere für Einmalbefragungen (z. B. auf Grundlage

einer Zufallsauswahl aus dem Telefonbuch), bei denen die erhobenen Angaben sofort bei der Erfassung anonymisiert werden. Telefonnummer und Name werden nicht gespeichert. Ihre Vernichtung erfolgt nachweisbar unmittelbar nach der Datenerhebung. Bis zur Vernichtung sind sie physisch getrennt und gesichert aufzubewahren. Auch kann es zulässig sein, die Telefonnummern getrennt für spätere Nach- oder Neubefragungen zu speichern, wenn der Betroffene beim Interview explizit mündlich zugestimmt hat, d. h. die Frage im Interviewleitfaden dokumentiert ist.

Soll hingegen mit Telefonbefragungen erst ein Vorinterview geführt werden, so ist bei der Hauptbefragung (durch Interviewer vor Ort beim Betroffenen) die schriftliche Einwilligung, wenn eine personenbezogene Speicherung erfolgen soll, nachzuholen. Wird im Unterschied dazu die Befragung codiert durchgeführt (z. B. mit Bogennummern) und lediglich auf einer getrennten Begehungliste zur Interviewerkontrolle Namen und Anschrift vermerkt, so kann ein Absehen von der Schriftform als angemessen angesehen werden, weil die mündliche Bereitschaft zur Befragung den Willen des Betroffenen klar zum Ausdruck bringt. Die Begehunglisten sind nach der Kontrolle zu vernichten (oder, wenn eine längere Aufbewahrungsfrist erforderlich ist, bei einem Datentreuhänder bis zur Vernichtung zu hinterlegen). Die Beratungspraxis der Datenschutzbeauftragten hat gezeigt, dass die Akzeptanz bei Telefoninterviews generell durch eine schriftliche Vorankündigung erhöht wird.

Auch bei mündlicher Einwilligung sind die Anforderungen an die umfassende Aufklärung des Betroffenen zu beachten (s. 4.2). In der Praxis wird bei „Haustürinterviews“ neben einer schriftlichen Vorankündigung auch eine Information zum Datenschutz an die Betroffenen übergeben, mit der diesen Anforderungen entsprochen wird.

Ein Absehen von der Schriftform ist in jedem Fall unzulässig, wenn eine bereichsspezifische Rechtsnorm ausschließlich die Schriftform der Einwilligung zulässt (s. z. B. § 5a Abs. 5 Berliner Schulgesetz, anders § 84 Abs. 2 Hessisches Schulgesetz).

4.5 Einwilligung bei nicht einwilligungsfähigen Personen

4.5.1 Grundsätzliches

Bei nicht einwilligungsfähigen Personen kann die Einwilligung keine rechtliche Wirksamkeit entfalten. Die Einwilligung ist eine rechtsgeschäftsähnliche Handlung, auf die die Vorschriften des Bürgerlichen Gesetzbuchs (BGB) über Willenserklärungen grundsätzlich entsprechend angewendet werden können. Die Einwilligungsfähigkeit richtet sich damit nach der natürlichen Einsichts-, Urteils- und Verstandesfähigkeit. Der Einwilligende muss in der Lage sein, die Tragweite des Eingriffs zu erkennen und das Für und Wider abzuwägen.

Im Grundsatz ist davon auszugehen, dass Minderjährige unter 14 Jahren nicht rechtswirksam in die Verarbeitung ihrer personenbezogenen Daten zu Forschungszwecken einwilligen können. Verbindliche Altersgrenzen können jedoch nicht generell festgelegt werden. Die Einwilligungsfähigkeit ist im Einzelfall unter Berücksichtigung der Schwere des Eingriffs zu beurteilen. Nach Art. 6 Abs. 2 Satz 1 GG üben die Eltern das Erziehungsrecht gegenüber dem Kind aus und tragen dafür die an Pflichten gebundene Verantwortung. Das elterliche Erziehungsrecht, das auch die Vertretung bei der Wahrnehmung des informationellen Selbstbestimmungsrechts für das Kind zunächst voll mit einschließt, schwindet über gesetzlich grob festgelegte Stufen bis zur Volljährigkeit. Die Grundrechtsträgereigenschaft einer Person beginnt spätestens mit der Geburt. Sobald die natürliche Einsichts-, Urteils- und

Verständnisfähigkeit es erlaubt, bestimmte Rechte selbst wahrzunehmen (z. B. Einsicht in Schülerunterlagen in Berlin), können sowohl die Eltern als auch die Jugendlichen selbst entscheiden. Wissenschaftliche Befragungen an Schulen hat der Berliner Gesetzgeber jedoch nur nach schriftlicher Einwilligung der Erziehungsberechtigten zugelassen. Hier wird der Umstand berücksichtigt, dass die Schüler aufgrund der gesetzlichen Schulpflicht die Schule besuchen und die Freiwilligkeit der Einwilligung der Schüler durch die Pflicht zur Anwesenheit (Schulbesuchspflicht) eingeschränkt sein kann. Jedoch kann aus einer Einwilligung durch die Eltern nicht auf eine Verpflichtung des Minderjährigen geschlossen werden, an der gewünschten Untersuchung teilzunehmen. Mit ihrer Einwilligung geben die Eltern zwar dem Wissenschaftler das Recht zur Datenerhebung, sie können damit jedoch das Recht des Minderjährigen auf Verweigerung seiner Mitwirkung nicht beschneiden. Verweigert ein Schüler beispielsweise die Teilnahme an einer Befragung, obwohl seine Eltern zugestimmt hatten, so ist dies Ausdruck des durch die Einwilligung auf den Schüler voll übertragenen Grundrechts und ist durch den Forscher zu akzeptieren.

Auch volljährige Personen können z. B. aufgrund einer vorübergehenden oder dauerhaften Erkrankung einwilligungsunfähig sein. Bei diesen Personen richtet sich die Einwilligungsfähigkeit nach der aktuell gegebenen Einsichts-, Urteils- und Verständnisfähigkeit. Die Bestellung eines Betreuers gemäß § 1896 Abs. 1 BGB lässt nach herrschender Meinung die Geschäftsfähigkeit und die Einwilligungsfähigkeit grundsätzlich unberührt. Die Bestellung eines Betreuers gibt aber Anlass, die Einwilligungsfähigkeit des Betreuten für einen bestimmten Eingriff sorgfältig zu prüfen.

Bei nicht einwilligungsunfähigen minderjährigen oder volljährigen Personen muss die Einwilligung des gesetzlichen Vertreters grundsätzlich zulässig und im Einzelfall rechtswirksam erteilt sein.

4.5.2 Spezialgesetzliche Regelungen

Das Arzneimittelgesetz (AMG) lässt klinische Forschung mit einwilligungsunfähigen Personen nur in beschränktem Umfang zu (§§ 40, 41 AMG). Rein wissenschaftliche, ausschließlich nichttherapeutische Arzneimittelversuche mit geschäfts- oder einwilligungsunfähigen Probanden sind – mit engen Ausnahmen für Pädiatrika – grundsätzlich unzulässig. Zulässig sind hingegen mit Einwilligung des gesetzlichen Vertreters Heilversuche mit ausschließlich therapeutischer Zielsetzung.

Die Regelungen des Medizinproduktegesetzes (MPG) sind weitgehend identisch mit denjenigen des Arzneimittelgesetzes (§§ 17, 18 MPG). Auch nach der Strahlenschutzverordnung ist nichttherapeutische Forschung mit geschäfts- oder einwilligungsunfähigen Personen unzulässig (§ 41 Abs. 6 Strahlenschutzverordnung).

4.5.3 Forschung außerhalb der spezialgesetzlich geregelten Bereiche

Außerhalb des Anwendungsbereichs der o. a. spezialgesetzlichen Regelungen sind die vorhandenen internationalen Erklärungen sowie die nationalen Stellungnahmen, Richtlinien und Empfehlungen (s. Anlage 5) und die Inhalte der spezialgesetzlichen Regelungen für die Interpretation der gegenwärtigen Rechtslage mit heranzuziehen. Bei nicht einwilligungsunfähigen minderjährigen oder volljährigen Personen ist die rechtlich zulässige und rechtswirksam erteilte Einwilligung des gesetzlichen Vertreters erforderlich. Sie verpflichtet diese allerdings nicht zur Mitwirkung, worüber sie aufzuklären sind.

Die Frage, inwieweit einem Betreuer i. S. v. § 1896 Abs. 1 BGB eine Befugnis zur Einwilligung in die Verwendung der Daten des Betreuten für ein Forschungsvorhaben zusteht, ist umstritten. Differenziert wird überwiegend zwischen therapeutischer und nichttherapeutischer Forschung, innerhalb der therapeutischen Forschung wird darüber hinausgehend danach differenziert, ob dem Betroffenen die Forschung im weiteren Verlauf der Krankheit oder bei einem späteren Wiederauftreten der Krankheit nutzen kann. Zumindest für Zwecke ausschließlich fremdnütziger Forschung wird ganz überwiegend die Verwendung der Daten des Betreuten auf der Grundlage einer Einwilligung des Betreuers als grundsätzlich unzulässig angesehen, teilweise auch für Zwecke therapeutischer Forschung, die dem Betroffenen nicht unmittelbar nützen kann. Im Übrigen kommt eine Einwilligung des gesetzlichen Betreuers in Betracht. Da sich die Betreuungsbestellung immer auf konkrete Aufgabenkreise beschränkt, die vom Vormundschaftsgericht nach dem Erforderlichkeitsgrundsatz konkret zu benennen sind, muss die Einwilligung in ein medizinisches Forschungsvorhaben in den Aufgabenkreis des Betreuers fallen.

Bei Minderjährigen sind im Normalfall die Eltern die gesetzlichen Vertreter (§ 1629 Abs. 1 Satz 1 BGB). Hinsichtlich der materiellen Entscheidungskompetenz gelten nach überwiegender Auffassung die gleichen Grundsätze wie bei einwilligungsunfähigen Volljährigen.

Sowohl bei einwilligungsunfähigen Volljährigen als auch bei partiell einwilligungsunfähigen Minderjährigen ist ein ablehnendes Verhalten der Betroffenen selbst nach überwiegender Auffassung angemessen zu berücksichtigen, in keinem Fall darf er zur Mitwirkung gezwungen werden.

5. Gesetzliche Regelungen zur Forschung mit personenbezogenen Daten ohne Einwilligung der Betroffenen

5.1 Grundsätzliches

Trotz der grundrechtlich gewährleisteten Forschungsfreiheit gilt auch für die wissenschaftliche Forschung mit personenbezogenen Daten wegen des Aufeinandertreffens zweier Grundrechte das grundsätzliche Verbot mit Erlaubnisvorbehalt. Rechtlich unproblematisch ist die Forschung mit anonymisierten Daten (fehlender Personenbezug) oder nach Einwilligung des Betroffenen (ausgeübtes informationelles Selbstbestimmungsrecht). Diese beiden Möglichkeiten allein würden aber eine Vielzahl von Forschungsvorhaben, für die oft ein erhebliches öffentliches Interesse besteht, verhindern. Daher hat der Gesetzgeber in Bund und Ländern besondere Erlaubnistatbestände für die Forschung geschaffen. Diese Forschungsregelungen (-klauseln, -privilegien) legen die rechtlichen Vorgaben fest, unter denen Einschränkungen des informationellen Selbstbestimmungsrechts zum Zwecke der wissenschaftlichen Forschung möglich sind (s. 5.2). Kern sind dabei Bedingungen, die eine Forschung ohne Einwilligung „hinter dem Rücken“ des Betroffenen erlauben.

Die in den gesetzlichen Forschungsregelungen aufgestellten Voraussetzungen weisen in ihren wesentlichen Inhalten einander ähnliche Regelungsmodalitäten auf. Einschränkung ist durchgängig zu beachten: Unterliegen Daten einem besonderen Amtsgeheimnis, so kann ihre Verarbeitung nicht auf die Forschungsregelungen des § 30 BlnDSG bzw. des § 33 HDSG gestützt werden. Hier kommen allein die speziellen Rechtsvorschriften als Rechtsgrundlage für Datenübermittlungen in Betracht, z. B. für Sozialdaten das Sozialgesetzbuch, für Daten aus dem Bereich der gesetzlichen Krankenversicherung speziell das Sozialgesetzbuch V, für Daten über Krebserkrankungen die Krebsregistergesetze und für statistische Daten das Bundes- und die Landesstatistikgesetze. Für den Bereich der medizinischen Forschung ist die ärztliche Schweigepflicht (§ 203 Abs. 1 StGB) und die ärztliche Berufsordnung zu beachten. Zum Zwecke der wissenschaftlichen Forschung dürfen der Schweigepflicht unterliegende Tatsachen und Befunde nur so weit mitgeteilt werden, als dabei die Anonymität des Patienten gesichert ist oder dieser ausdrücklich zustimmt oder eine gesetzliche Forschungsregelung vorliegt, die als Befugnis zur Offenbarung der Schweigepflicht unterliegender Daten qualifiziert werden kann. Für andere Berufsgeheimnisse gilt Entsprechendes.

Häufig wird in den spezialgesetzlichen Forschungsklauseln nicht das gesamte Verfahren festgelegt. Dann sind ergänzend die Vorschriften der Landesdatenschutzgesetze oder des Bundesdatenschutzgesetzes herbeizuziehen.

5.2 Rechtliche Vorgaben von Forschungsregelungen am Beispiel von § 30 BlnDSG und § 33 HDSG

Möchte ein Forscher personenbezogene Daten, die von einer öffentlichen Stelle für einen anderen Zweck erhoben wurden, ohne Einwilligung des Betroffenen für ein Vorhaben verwenden, so muss das Vorhaben den rechtlichen Voraussetzungen der gesetzlichen Forschungsregelungen genügen. Der Forscher hat das Vorliegen dieser rechtlichen Voraussetzungen in einem Antrag auf Übermittlung der Daten darzulegen. Nur so kann entschieden

werden, ob der mit der Übermittlung der Daten an die Forschung verbundene Grundrechtseingriff eine gesetzliche Grundlage hat und verhältnismäßig ist. Die rechtliche Verantwortung für die Zulässigkeit der Übermittlung trägt immer die Stelle, die die Daten für den ursprünglichen Zweck erhoben hat, ggf. auch die genehmigende übergeordnete Stelle. Sie hat die rechtlichen Vorgaben zu prüfen.

5.2.1 *Konkretes Forschungsvorhaben*

Das Forschungsvorhaben muss grundsätzlich schon vor einer Übermittlung der Daten an den Forscher hinreichend konkretisiert sein. In der Praxis hat sich allerdings gezeigt, dass es bei einzelnen Forschungsvorhaben später wichtig werden kann, die bereits erhaltenen Daten für die Bearbeitung neuer oder veränderter Fragestellungen zu nutzen, die zum Zeitpunkt des Antrags auf Übermittlung der Daten noch nicht bekannt waren und daher in den Antrag nicht einbezogen wurden. Ein erneuter Antrag wäre oft nicht möglich oder mit zusätzlichem hohem Aufwand und Kosten und Problemen der Repräsentativität der Daten verbunden. Im Hinblick auf die Eigengesetzlichkeiten der wissenschaftlichen Arbeitsweise erscheint es vertretbar und angemessen, den Zweck der Übermittlung der Daten (d. h. die Darstellung des Forschungsvorhabens) so zu formulieren, dass evtl. nicht substanzielle inhaltliche Änderungen oder Ausweitungen der Fragestellungen der Studie mit umfasst sind. Die das Forschungsvorhaben durchführende Stelle muss in dem Antrag auf Übermittlung der personenbezogenen Daten konkret und verbindlich benannt werden. In die Studie einbezogene Kooperationspartner müssen aufgeführt werden, soweit sie mit einer eigenständigen Verarbeitung der personenbezogenen Daten befasst werden.

5.2.2 *Wissenschaftliches Forschungsvorhaben*

Die Forschungsregelungen beruhen auf einem grundsätzlichen Nutzungsverbot mit Erlaubnisvorbehalt. Dieses grundsätzliche Nutzungsverbot würde unterlaufen, wenn jede Forschung in einem beliebigen wirtschaftlichen oder sozialen Kontext das Verbot außer Kraft setzen würde. „Wissenschaftlich“ im Sinne der Forschungsklausel ist nur eine rein wissenschaftliche Tätigkeit, die weder wirtschaftlichen noch sonstigen nicht wissenschaftlichen Interessen untergeordnet ist. Voraussetzung ist die Unabhängigkeit des Forschers oder der Forschungseinrichtung. Hinsichtlich der konkreten Tätigkeit, für welche die Daten genutzt werden sollen, darf keine Weisungsabhängigkeit bestehen. Wissenschaftlich tätig ist damit – neben den Hochschulen – auch eine Reihe weiterer unabhängiger wissenschaftlicher Einrichtungen (z. B. Max-Planck-Gesellschaft). Auch privatrechtlich konstituierte Forschungseinrichtungen (z. B. Stiftungen) können diese Voraussetzungen erfüllen. Dies gilt auch für unabhängige Forschungseinrichtungen, die im Auftrag von Wirtschaftsunternehmen tätig werden. Ob sonstige Unternehmensforschung wissenschaftlichen Zwecken im o. g. Sinne dient, ist im Einzelfall zu prüfen.

5.2.3 *Keine Beeinträchtigung schutzwürdiger Belange der Betroffenen*

Nach § 30 BlnDSG bzw. § 33 HDSG dürfen öffentliche Stellen ohne die Einwilligung des Betroffenen für bestimmte Forschungsarbeiten Daten übermitteln, wenn schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Eine Beeinträchtigung schutzwürdiger Belange kann im Einzelfall ausgeschlossen sein wegen

- der Art der Daten oder
- der Offenkundigkeit der Daten (d.h. der Inhalt dieser Daten ist ohne Probleme jedermann zugänglich). Wenn die Angaben zwar zu einem zurückliegenden Zeitpunkt offenkundig waren, aber zum Zeitpunkt der Forschung weitgehend in Vergessenheit geraten sind, ist diese Voraussetzung häufig nicht mehr gegeben (s. „Lebach-Urteil“ des BVerfGE 35, 202 [232]),
- der Art der Verwendung; der Verwendungszweck berührt z. B. in keiner Weise schutzwürdige Belange der Betroffenen, wenn die Daten im Rahmen eines Adressmittlungsverfahrens (s. unten 6.1) verarbeitet werden und wenn sie durch die Daten besitzende Stelle selbst oder im Auftrag anonymisiert werden.

Diese Konstellationen werden jedoch nur in Ausnahmefällen vorliegen, da wissenschaftliche Forschungsvorhaben häufig tief greifende und differenzierte personenbezogene Angaben erfordern. Angesichts hoher Datendichte ist überwiegend von einer Beeinträchtigung schutzwürdiger Belange der Betroffenen auszugehen.

5.2.4 Alternativ: Überwiegendes öffentliches Interesse an der Durchführung des Forschungsvorhabens

Öffentliche Stellen dürfen nach § 30 BlnDSG bzw. § 33 HDSG ohne Einwilligung des Betroffenen für bestimmte Forschungsarbeiten Daten auch übermitteln, wenn ein öffentliches Interesse an der Durchführung des Forschungsvorhabens besteht und dieses die schutzwürdigen Belange des Betroffenen überwiegt. Weitere Voraussetzungen sind in diesem Fall, dass der Forschungszweck nicht auf andere Weise erreicht werden kann und eine Zustimmung der obersten Landesbehörde erfolgt.

Nicht jedes wissenschaftliche Interesse an der Durchführung eines Forschungsvorhabens kann gegenüber dem Geheimhaltungsinteresse eines Betroffenen ohne weiteres Vorrang haben. Das Ergebnis der notwendigen Abwägung im Rahmen praktischer Konkordanz (s. 1.) ist offen. Ein überwiegendes Forschungsinteresse ist dann gegeben, wenn an der Durchführung des Forschungsvorhabens ein öffentliches Interesse besteht und der Eingriff in die Rechte des Betroffenen infolge einer datenschutzgerechten Ausgestaltung des Forschungsvorhabens so gering wie möglich gehalten wird und nicht außer Verhältnis zu dem angestrebten Zweck steht. Dies ist durch den Forscher im Rahmen eines Forschungsdesigns (Hypothesen, methodische Anlage und Durchführung, Alternativenbeschreibung, datenschutzrechtliche Absicherung, Darlegung, warum nicht mit anonymisierten oder pseudonymisierten Daten gearbeitet werden kann) im Einzelfall darzulegen. Ein überwiegendes öffentliches Interesse an der Durchführung des Forschungsvorhabens kann nur dann bejaht werden, wenn verlässliche wissenschaftliche Forschungsergebnisse zu erwarten sind und das Forschungsvorhaben keinen gesetzlichen oder verfassungsrechtlichen Vorgaben widerspricht.

Ein die schutzwürdigen Belange der Betroffenen überwiegendes öffentliches Interesse an dem Forschungsvorhaben ist bei Examens-, Diplomarbeiten etc., die zunächst dem Nachweis der wissenschaftlichen Qualifikation dienen, u. a. auch deshalb problematisch, weil hier Kandidaten als Privatpersonen handeln, die Doktorarbeit oder Diplomarbeit vielfach in ihrer Privatwohnung schreiben und insgesamt die erforderlichen organisatorischen und verfahrensrechtlichen Vorkehrungen zum Schutz der Daten kaum sicherstellen können. Diese Einschränkungen gelten auch für einen Teil der Dissertationen. Anders ist es, wenn eine Forschungseinrichtung, z. B. ein Universitätsinstitut, vertreten durch den die Dissertation

betreuenden Doktorvater, als Daten besitzende Stelle auftritt oder schriftlich bestätigt, dass Räume zur Verfügung gestellt und die Einhaltung der organisatorischen und verfahrensrechtlichen Vorkehrungen zum Schutz der Daten gewährleistet wird. Ein öffentliches Interesse bei einer Dissertation kann insbesondere angenommen werden, wenn die Arbeit Teil eines größeren Forschungsvorhabens ist und/oder ein Stipendium (z. B. der DFG, Sonderforschungsbereich) oder aufgrund der Prüfung einer anerkannten wissenschaftlichen Institution Mittel hierfür bereitgestellt werden.

5.2.5 *Keine Möglichkeit, den Zweck der Forschung auf andere Weise zu erreichen*

Eine Verarbeitung personenbezogener Daten für ein Forschungsvorhaben auf der Grundlage einer gesetzlichen Forschungsregelung kommt ohne Einwilligung der Betroffenen nur dann in Betracht, wenn der Forschungszweck nicht auf andere Weise erreicht werden kann. Vorrangig ist stets zu prüfen, ob das Vorhaben nicht mit anonymisierten bzw. pseudonymisierten Daten oder mit Kombinationsformen des Datenzugangs durchgeführt werden kann und ob es nicht zumutbar ist, eine Einwilligung der Betroffenen einzuholen (s. 1).

Die Einholung der Einwilligung der Betroffenen ist nur dann verzichtbar, wenn

- der Aufenthalt des Betroffenen unbekannt ist oder andere Umstände es ausschließen, mit ihm Verbindung aufzunehmen (projektgefährdender Zeitverzug, unverhältnismäßiger Aufwand),
- die Einholung der Einwilligung für den Betroffenen unzumutbar ist. Das ist anzunehmen, wenn die Einholung den Betroffenen subjektiv in unerträglicher Weise belasten würde, insbesondere durch die von ihm dann zu treffende Entscheidung zwischen Einwilligung und Verweigerung. Unzumutbar sind Ersuchen, wenn durch die Einholung der Einwilligung dem Betroffenen Erkenntnisse offenbart werden müssten, mit denen er vermutlich nicht (mögliche Erkrankung, genetische Disposition) oder nicht mehr konfrontiert werden will (Straftaten),
- durch das Einholen der Einwilligung der Forschungszweck eindeutig gefährdet wird. Bei Einholung der Einwilligung muss oft mit einer Verweigerung gerechnet werden, wenn dem Betroffenen die Ergebnisse der Forschung (etwa über seine Beteiligung an Ereignissen der Zeitgeschichte) unangenehm sein werden,
- das Forschungsergebnis nur durch eine „Totalzählung“ erreicht werden kann.

Die Ausnahmetatbestände der § 30 BlnDSG und § 33 HDSG rechtfertigen es jedoch nicht, schon dann von der Einholung der Einwilligung abzusehen, wenn es schwierig wird, eine informierte Einwilligung des Betroffenen zu erreichen. Eine Alternative kann darin liegen, mit kleineren Stichproben oder einem veränderten Forschungsdesign zu arbeiten. Auch ein gesteigerter Verwaltungsaufwand allein kann das Absehen von einer Einwilligung nicht rechtfertigen; nur bei unzumutbar hohen Kosten oder unzumutbarem Verwaltungsaufwand, etwa für die Ermittlung der Adressen, und gering belastender Datendichte kann der Aufwand unter Berücksichtigung des öffentlichen Interesses (s. 5.2.4) Ausnahmen rechtfertigen.

Die Durchführung eines Forschungsvorhabens, das die Erstellung von Persönlichkeitsbildern, die Verarbeitung intimer Angaben, Selbstbezeichnungen oder Daten, die die Gefahr einer sozialen Diskriminierung mit sich bringen, zum Gegenstand haben soll, wird vielfach als ein unverhältnismäßiger Eingriff in die Interessen der Betroffenen qualifiziert werden müssen.

Der rechtsstaatliche Grundsatz des Vertrauensschutzes verbietet es regelmäßig, § 30 Abs. 1 BlnDSG bzw. § 33 HDSG anzuwenden und Daten ohne Einwilligung zu verarbeiten, wenn der Betroffene zuvor nach § 6 Abs. 2 BlnDSG bzw. § 7 HDSG die Einwilligung ausdrücklich verweigert hat. Ausnahmen werden nach Verweigerung nur gemacht werden können, wenn ein besonderes, jetzt anders nicht mehr wahrnehmbares öffentliches Interesse an den Forschungsdaten besteht.

Auch bei der Verarbeitung sensibler Daten i. S. d. Art. 8 EG-RL muss ein besonders gewichtiges Interesse an der Durchführung des Forschungsvorhabens vorliegen, wenn von der Einholung der Einwilligung des Betroffenen abgesehen werden soll.

5.2.6 Zustimmung der obersten Landesbehörde

Die in den gesetzlichen Regelungen geforderte Zustimmung der obersten Landesbehörde muss eindeutig bezeichnen:

- den Empfänger der Daten,
- die Art der zu übermittelnden personenbezogenen Daten (Inhalt und vorliegende Form, z.B. Akten),
- den Kreis der Betroffenen (qualitativ und quantitativ zu benennen),
- die genaue Bezeichnung des Forschungsvorhabens,
- die im Einzelfall genehmigten Modalitäten der Verwendung der Daten.

Diese Zustimmung ist dem Berliner bzw. dem Hessischen Datenschutzbeauftragten mitzuteilen. In der Praxis der vergangenen Jahre hat es sich als günstig für die zeitnahe Realisierung von Forschungsvorhaben erwiesen, wenn sich Forscher im Vorfeld einer beantragten Zustimmung durch die oberste Landesbehörde mit dem Berliner bzw. dem Hessischen Datenschutzbeauftragten in Verbindung gesetzt und sich von diesem bezüglich der datenschutzgerechten Gestaltung des Forschungsvorhabens beraten lassen.

§ 30 Abs. 1 BlnDSG und § 33 HDSG sehen keine Verpflichtung der öffentlichen Stelle zur Datenübermittlung vor, die Datenübermittlung steht vielmehr im pflichtgemäßen Ermessen dieser Stelle. Selbst die Erteilung der Zustimmung der obersten Landesbehörde zieht nicht zwingend die Datenübermittlung zum Zwecke wissenschaftlicher Forschung nach sich.

5.2.7 Zweckbindung der Daten

Nach § 30 Abs. 3 BlnDSG bzw. § 33 Abs. 3 HDSG unterliegen die übermittelten Daten einer strikten Zweckbindung. Der Empfänger darf sie nur für das ausdrücklich bezeichnete Forschungsvorhaben verwenden (vgl. auch § 28 Abs. 4 Meldegesetz Berlin). Für die einem besonderen Amtsgeheimnis unterliegenden Daten ist die Zweckbindung beispielsweise in § 78 Satz 1 SGB X und § 16 Abs. 3 Satz 1 Bundesstatistikgesetz festgelegt.

5.2.8 Trennungs- und Löschungsgebot

§ 30 Abs. 2 BlnDSG bzw. § 33 Abs. 2 HDSG verpflichtet die Stellen, die zu wissenschaftlichen Zwecken personenbezogene Daten verarbeiten, zu einer möglichst frühen Anonymisierung. Die Daten sind so bald wie möglich dahin zu verändern, dass ein Bezug auf eine

bestimmte Person nicht mehr erkennbar ist. Merkmale, mit denen dieser Bezug wiederhergestellt werden kann, sind gesondert zu speichern (Trennungsgebot). Personenbezogene Daten sind zu löschen, sobald der Forschungszweck dies gestattet, spätestens jedoch, sobald der Forschungszweck erreicht ist. Eine längere Speicherdauer ist nur zu rechtfertigen, wenn die Daten anonymisiert werden (s. aber 7.1 zur längerfristigen Speicherung der Daten zur Sicherung guter wissenschaftlicher Praxis).

5.2.9 Kontrollmöglichkeit

§ 30 Abs. 4 BlnDSG bzw. § 33 Abs. 4 HDSG macht eine Übermittlung an Stellen außerhalb des Anwendungsbereichs des Landesrechts (öffentliche Stellen des Bundes oder eines anderen Bundeslandes sowie nicht-öffentliche Stellen und Personen) möglich, aber auch von zusätzlichen Voraussetzungen abhängig. Sie ist nur zulässig, wenn sich der Empfänger verpflichtet, die Zweckbindung sowie das Anonymisierungs-, Trennungs- und Lösungsgebot zu beachten und sich der Kontrolle des Berliner Beauftragten für Datenschutz und Informationsfreiheit bzw. des Hessischen Datenschutzbeauftragten zu unterwerfen. Damit werden sog. „kontrollfreie“ Räume verhindert.

5.2.10 Veröffentlichung der Daten

§ 30 Abs. 5 BlnDSG enthält eine spezielle Regelung für die Veröffentlichung personenbezogener Daten durch wissenschaftliche Forschung betreibende öffentliche Stellen. Sie ist nur zulässig, wenn entweder der Betroffene eingewilligt hat oder die Veröffentlichung für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist. Diese Vorschriften verbieten jede anderweitige Veröffentlichung personenbezogener Daten und schließen damit eine Veröffentlichung auf der Grundlage der Übermittlungsbefugnis nach § 30 Abs. 1 BlnDSG aus.

Mit § 30 Abs. 5 BlnDSG ist eine gesetzliche Grundlage für die Veröffentlichung personenbezogener wissenschaftlicher Forschungsergebnisse über Ereignisse der Zeitgeschichte ohne Einwilligung des Betroffenen geschaffen worden. Eine öffentliche Aufarbeitung zeitgeschichtlicher Ereignisse soll im Einzelfall auch gegen den Willen der betroffenen Personen möglich sein. Solche Eingriffe in das informationelle Selbstbestimmungsrecht sind allerdings nur insoweit gerechtfertigt, als eine personenbezogene Veröffentlichung für die Darstellung von zeitgeschichtlichen Forschungsergebnissen unerlässlich ist. Dagegen gebietet der verfassungsrechtliche Grundsatz des Übermaßverbotes, das Geheimhaltungsinteresse von Opfern und Benachteiligten zu beachten und deren personenbezogene Daten nur mit ihrer Einwilligung zu veröffentlichen. Inwieweit eine Person als eine Person der Zeitgeschichte gilt, ist durch ihren eigenen Anteil an der öffentlichen Bedeutung des Ereignisses zu beurteilen (s. 7.4). Die personenbezogene Veröffentlichung muss aber in jedem Fall unerlässlich für die Darstellung des Ereignisses sein. Werden hingegen typische Lebenswege oder Gruppenschicksale geschildert, so ist eine anonymisierte Darstellung geboten. Anders ist es, wenn ohne die namentliche Bezeichnung der konkreten Person das Forschungsergebnis nicht mehr verständlich wäre.

In Hessen ist die Zulässigkeit der Veröffentlichung personenbezogener Daten einzubeziehen in die Prüfung, ob schutzwürdige Belange der Betroffenen beeinträchtigt werden (s. 5.2.3) oder ein überwiegendes öffentliches Interesse an der Durchführung des Forschungsvorhabens (s. 5.2.4) besteht.

5.2.11 Eigenforschung

Mit § 30 Abs. 6 BlnDSG und § 33 Abs. 1 HDSG wird es Personen, die innerhalb einer öffentlichen Stelle Zugriff auf den dortigen Datenbestand haben, erlaubt, personenbezogene Daten ohne Einwilligung für Forschungszwecke zu verarbeiten, soweit ihre Zuständigkeit das gestattet (interne Forschung, Eigen- oder Inhouse-Forschung). Damit wird öffentlichen Stellen die Nutzung interner Quellen zu Forschungszwecken ermöglicht. Die Belastung der Betroffenen ist in diesem Falle geringer, weil im Regelfall keine zusätzliche Erhebung und Übermittlung stattfindet, so dass in der Verarbeitung nur ein begrenzter zusätzlicher Eingriff liegt. Die gesetzliche Regelung hat es für vertretbar gehalten, die mit der Verwendung der Daten für Forschungszwecke verbundene Zweckänderung auch ohne Einwilligung des Betroffenen zuzulassen. Der Forschungszweck darf jedoch nicht auf andere Weise – insbesondere auch ohne personenbezogene Daten – erreicht werden können. Auch hier ist eine Interessenabwägung erforderlich: Das Interesse der Betroffenen an der Zweckbindung der Daten darf das öffentliche Interesse an der Zweckänderung zur Durchführung des Forschungsvorhabens nicht überwiegen.

5.2.12 Resümee

Die Regelungen des § 30 BlnDSG und § 33 HDSG, die unter bestimmten Voraussetzungen eine Verwendung von zu anderen Zwecken erhobenen Daten in Forschungsvorhaben – d. h. eine Zweckänderung – zulassen, enthalten detaillierte Vorgaben hinsichtlich der Weiterverarbeitung der Daten zu Forschungszwecken, die als „geeignete Garantien“ i. S. v. Art. 6 Abs. 1b EG-RL qualifiziert werden können (vgl. oben 2.). Gemäß Art. 11 Abs. 2 EG-RL besteht in diesen Fällen keine Verpflichtung zur Information der Betroffenen. Das Auskunftsrecht der Betroffenen bleibt allerdings unberührt.

6. Kombinationsformen des Datenzugangs

Die „klassischen“ und „reinen“ Formen des Datenzugangs für den Wissenschaftler liegen in der Nutzung anonymisierter bzw. pseudonymisierter Daten, mit Einwilligung erhobener Daten und im Datenzugang auf Grundlage einer gesetzlichen Forschungsregelung. Die zwingende Verpflichtung zur Beachtung des Verhältnismäßigkeitsgrundsatzes und damit zur Wahl des mildesten Mittels zwingt stets zur Prüfung, ob bei fehlender Einwilligung nicht auf die Verarbeitung personenbezogener Daten zu Gunsten anonymisierter oder pseudonymisierter Daten verzichtet werden kann, ob mit verminderten Datensätzen auszukommen ist oder ob die datenschutzrechtlichen Sicherungen auf andere Weise erhöht werden können (durch Datentreuhänder oder durch Verarbeitung an „neutraler“ Stelle). Die Suche nach der schwächsten Form des Grundrechtseingriffs führt in der Praxis zu verschiedenen aus der Spezifik des Forschungsvorhabens resultierenden Kombinationen und Mischformen. Sie sind deutlichster Ausdruck der Lösung der Grundrechtskollision auf dem Wege der praktischen Konkordanz (s. 1.).

6.1 Das Adressmittlungsverfahren

Aus verschiedensten Anlässen treten Privatpersonen, aber auch wissenschaftliche Institutionen an Hochschulen an andere Bildungseinrichtungen, Behörden, Kammern usw. heran und bitten, ihnen Adressen von Absolventen, Betreuten oder Mitgliedern zu überlassen. Dies betrifft u. a. angestrebte wissenschaftliche Studien ebenso wie die Vorbereitung beabsichtigter Absolvententreffen. In diesen Fällen ist, wenn keine spezielle gesetzliche Regelung besteht, grundsätzlich nach § 6 BlnDSG i. V m. §§ 12 bzw. 13 oder 14 BlnDSG bzw. § 7 Abs. 1 Nr. 1, 3 HDSG zu verfahren. Ist jedoch vor der Nutzung der Adresse für andere als die ursprünglichen Zwecke der Speicherung keine Einwilligung einholbar oder ist die Nutzung der Adresse gerade die zwingende Voraussetzung für das Einholen der Einwilligung, so bietet sich zur Lösung des Konfliktes das Adressmittlungsverfahren an.

Beim Adressmittlungsverfahren werden beispielsweise den Bildungseinrichtungen frankierte, aber nicht adressierte Briefumschläge sowie das zu versendende Material übergeben. Die Bildungseinrichtung adressiert die Umschläge aufgrund der ihr vorliegenden Adressen und übergibt sie dem Postweg. Natürlich sollte der Angeschriebene in dem Begleitschreiben über dieses Verfahren aufgeklärt werden, damit er sichergehen kann, dass seine persönlichen Angaben nicht an Dritte weitergegeben wurden. Als Absender ist die Bildungseinrichtung anzugeben, um zu verhindern, dass bei Unzustellbarkeit Namen und (frühere) Anschriften doch noch ohne Einwilligung übermittelt werden. Es wäre – aus Gründen der Rationalität – zu empfehlen, im Rahmen der Datenverarbeitungsprojekte derartige Adressenausdrucke vorzusehen, wobei die Ausdrucke zu protokollieren sind. Auch ist es möglich, in bestimmten begründeten Fällen den gleichen Personenkreis ein zweites Mal anzuschreiben, um eine höhere Antwortquote zu erreichen. Von manchen Einrichtungen werden die Forscher insbesondere bei Vorhaben von besonderem öffentlichem Interesse auch insoweit unterstützt, als bei Unzustellbarkeit von den Meldebehörden die aktuelle Anschrift eingeholt und der Versand – wie oben beschrieben – wiederholt wird. Werden z. B. Adressen ohne das Adressmittlungsverfahren ausnahmsweise auf der Grundlage von § 30 Abs. 1 BlnDSG

bzw. § 33 HDSG für Forschungszwecke ohne Einwilligung der Betroffenen an Forschungseinrichtungen übermittelt, so muss die Forschungseinrichtung dies dem Betroffenen bereits bei der ersten Kontaktaufnahme (z. B. Befragung) mitteilen und erläutern. Je transparenter für den Betroffenen der Umgang des Forschers mit seinen personenbezogenen Daten wird, desto eher wird der Betroffene bereit sein, mit dem Forscher bei der anschließenden Befragung oder sonstigen Datenerhebung auf freiwilliger Basis zusammenzuarbeiten. Durch das Adressmittlungsverfahren wird vermieden, dass die Adressen der Betroffenen Dritten zur Kenntnis gelangen. Dieses Verfahren ist datenschutzrechtlich unbedenklich und sichert dem Betroffenen sein Recht auf informationelle Selbstbestimmung in vollem Umfang.

6.2 Datentreuhänder

6.2.1 *Die Grundidee*

Mit dem Einsatz von Datentreuhändern (auch als Vertrauensstellen bezeichnet) 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. Der Datentreuhänder übernimmt die Rolle eines vertrauenswürdigen Dritten. Er tritt zwischen die Daten besitzende öffentliche Stelle und den Forscher oder – in einer anderen Konstellation – zwischen den Betroffenen und den Forscher und sichert dadurch die Rechte Betroffener.

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. Der Datentreuhänder sollte an eine besondere Schweigepflicht gebunden sein. Bedauerlicherweise fehlen bislang gesonderte gesetzliche Regelungen, die die Vertrauenswürdigkeit eines Datentreuhänders explizit absichern.

Voraussetzung eines funktionsfähigen Datentreuhänders ist vor allem seine Vertrauenswürdigkeit und Unabhängigkeit. Gegenüber dem Betroffenen sowie der Daten besitzenden Behörde muss rechtlich und technisch-organisatorisch gewährleistet werden, dass nur der Datentreuhänder einen Personenbezug bei den Daten herstellen kann, die ihm von der Daten besitzenden Stelle oder mitunter auch vom Betroffenen selbst übermittelt worden sind. Chipkartensysteme bieten hierfür neue technische Möglichkeiten. In welchem Umfang und auf welche Weise er die Daten verarbeitet, ist vor Beginn des Forschungsvorhabens zwischen den Beteiligten vertraglich festzulegen. Der Forscher ist verpflichtet, die ihm übermittelten Daten zweckgebunden zu verwenden und gegen Missbrauch zu sichern. Nach der durch den Datentreuhänder erfolgenden Anonymisierung/Pseudonymisierung sollten die zu verarbeitenden Daten nicht beim Datentreuhänder aufbewahrt werden, sondern lediglich die Identifikationsdaten und Verschlüsselungsalgorithmen.

In der Vergangenheit wurden in der medizinischen Forschung Lösungen bevorzugt, bei denen Ärzte mit Verweis auf ihre Schweigepflicht als Treuhänder eingesetzt wurden und über getrennt verwahrte Identifikationsdaten (Namen und Anschrift) wachten. Aufgrund von nicht auszuschließenden Eigeninteressen der Ärzte kommt eine solche Lösung jedoch nicht immer in Betracht, außerdem ist umstritten, ob die ärztliche Schweigepflicht Anwendung findet, wenn der Arzt die Daten nicht im Rahmen eigener Behandlung, sondern im Rahmen eines Forschungsvorhabens zur Kenntnis erhält.

Für die Übermittlung personenbezogener Daten an einen Datentreuhänder gelten die rechtlichen Vorgaben der Forschungsregelungen (s. 4. und 5.). Grundsätzlich sollte auf der Grundlage einer informierten Einwilligung der Betroffenen der Datentreuhänder eingeschaltet werden. Ist dies nicht möglich, kommt eine Übermittlung der personenbezogenen Daten an den Treuhänder auf der Grundlage einer gesetzlichen Forschungsregelung in Betracht.

Die Daten besitzende Stelle ist gehalten, das aus Art. 5 Abs. 3 GG abgeleitete datenschutzrechtliche Wissenschaftsprivileg durch geeignete Maßnahmen zu unterstützen und zu fördern. Dies heißt nicht, dass für den Forscher ein verfassungsunmittelbares Datenzugangsrecht besteht. Für den Staat und damit für öffentliche Stellen besteht lediglich die Aufgabe, den Datenzugang zu fördern. Daraus lässt sich für die Daten besitzende Stelle die Befugnis ableiten, bei datenschutzgerechter Ausgestaltung des gesamten Verfahrens eine Übermittlung an einen Datentreuhänder zu erlauben. Eine derartig privilegierte Nutzung entbindet trotz Zwischenschaltung eines Datentreuhänders nicht davon, kombiniert weitere den Eingriff mildernde Maßnahmen wie die getrennte Speicherung der Identifikationsdaten oder/und eine anschließende Pseudonymisierung vorzugeben. Ein Datentreuhänder führt keine Datenverarbeitung im Auftrag i. S. d. § 3 BlnDSG und § 4 HDSG aus. Mit der dort geregelten weisungsgebundenen Auftragsdatenverarbeitung würde der Status des Datentreuhänders als vertrauenswürdiger Dritter verfehlt. Der Treuhänder ist selbständige Daten besitzende Stelle.

Wie mit Hilfe eines Datentreuhänders die Rechte der Betroffenen weniger beeinträchtigt werden, ob also das mildeste Mittel gewählt wird, ist anhand der einzelnen, ihm möglicherweise zu übertragenden Funktionen, die im Folgenden dargestellt werden, zu prüfen.

6.2.2 Anonymisierung/Pseudonymisierung der Daten durch den Treuhänder

In dieser Funktion wird der Datentreuhänder zwischen die Daten besitzende Stelle und Forscher gestellt, 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.

6.2.3 Verknüpfung der Daten durch den Treuhänder

Ist es erforderlich, später Daten aus verschiedenen Quellen oder unterschiedlichen Zeitpunkten oder unter verschiedenen Pseudonymen verborgene Daten derselben Person unter Nutzung eines Verschlüsselungsverfahrens (wieder) miteinander zu verknüpfen, so bestehen die geringsten verfassungsrechtlichen Einwände, wenn dies durch einen sachlich unbeteiligten Dritten geschieht. Dafür bietet sich der Datentreuhänder an. Er kann die verschiedenen Datensätze personenbezogen zusammenführen, anschließend erneut anonymisieren oder pseudonymisieren und in dieser Form an die beteiligten Forscher übermitteln. Der Datentreuhänder kann auch mehrere unterschiedliche Dateien personenbezogen verknüpfen und ggf. nach bestimmten Kriterien auswerten oder später neue Daten den Einzeldatensätzen zuordnen (linking). Er sichert somit entstehende Persönlichkeits(teil)bilder nach außen ab.

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. Das ist der Fall, wenn die Daten besitzende Stelle, deren Daten miteinander verknüpft werden sollen, ihre Daten nach einem nur bekannten und gleich lautenden Schlüssel an den Datentreuhänder übermittelt. Der Datentreuhänder kann dann die Daten trotz der ihm unbekannten Verschlüsselung miteinander verknüpfen. Soweit das verschlüsselte Ergebnis ausreichend anonymisiert bleibt, kann es in dieser Form an eine Forschungseinrichtung übermittelt werden. Denkbar ist auch ein Konstrukt, bei dem der Datentreuhänder lediglich Identifikationsdaten erhält, für die er dann unterschiedlichen Daten besitzenden Stellen Pseudonyme übermittelt. Die bei der Daten besitzenden Stelle pseudonymisierten Einzeldaten könnten unter besonderen Auflagen den Forschern direkt – also ohne dass beim Treuhänder erst der vollständige nichtanonymisierte Datenbestand gesammelt wird – übermittelt werden.

Angesichts der Problematik von Verknüpfungen und Zuordnungen personenbezogener Daten spricht das besondere Schutzbedürfnis der Betroffenen den Einsatz von Datentreuhändern. Der Datentreuhänder ist gegenüber einer direkten Übermittlung personenbezogener Daten an die Forschungseinrichtung ein milderes Mittel, weil die Daten nur bei ihm personenbezogen sind. Bei Längsschnittstudien können die Identifizierungsmerkmale beim Datentreuhänder verbleiben, so dass zu späteren Zeitpunkten beim Treuhänder, nicht aber bei der forschenden Stelle erneut personenbezogene Zuordnungen mit neuen Daten vorgenommen werden können.

6.2.4 Datenerhaltung, -bereitstellung und -archivierung durch den Treuhänder

Der Datentreuhänder hält personenbezogene Datenbestände als Datenbank oder Archiv für weitere Forschungszwecke vorrätig. Der Datentreuhänder kann auch die Funktion der Errichtung und Betreuung von Forschungsregistern, in denen personenbezogene Daten zu Forschungszwecken auf Vorrat gehalten werden, ausüben. Derartige Datensammlungen sind aber gegenüber der unmittelbar personenbezogenen Übermittlung an Einzelforscher auf Grundlage gesetzlicher Forschungsklauseln kein milderes Mittel. Es besteht mit Blick auf das informationelle Selbstbestimmungsrecht kein Unterschied, ob eine bestimmte Stelle oder ein Datentreuhänder durch Gesetz berechtigt wird, ein Forschungsregister zu führen. Außerdem können auf der Grundlage einer Forschungsklausel personenbezogene Daten nur im Einzelfall ohne Einwilligung des Betroffenen übermittelt und verarbeitet werden, während in Forschungsregistern personenbezogene Daten auf Vorrat gehalten werden, obwohl wie bei der amtlichen Statistik eine konkrete Zweckbindung nicht vorgegeben werden kann. Lediglich die erhöhte Beschlagnahmefestigkeit bei einem Anwalt oder Notar mildert den Eingriff etwas.

Anders verhält es sich, wenn statt einer Löschung der Einzeldaten nach Abschluss des Forschungsvorhabens die Einzeldaten zum Zwecke der wissenschaftlichen Überprüfbarkeit – getrennt nach Hilfs- und Erhebungsmerkmalen – bei zwei Treuhändern für einen bestimmten Zeitraum hinterlegt werden (s. 7.1).

6.2.5 Beispiel: Das Projekt QuaSi-Niere

Ein Beispiel für den Einsatz eines Treuhänders ist das Qualitätssicherungsprojekt QuaSi-Niere. Durch eine bundesweite Erfassung und Auswertung der Behandlungsdaten von Dialysepatienten und Transplantierten soll die medizinische Versorgung dieser Patienten-

gruppe verbessert werden. Auf der Grundlage einer Einwilligung der Patienten (s. Anlage 1 Beispiel 3) übermittelt der jeweils behandelnde Arzt die personenbezogenen Patientendaten an einen Treuhänder. Der Treuhänder generiert für jeden Patienten ein Pseudonym. Die medizinischen Behandlungsdaten werden ohne Identifikationsdaten mit dem vom Treuhänder generierten Pseudonym an die Projektgeschäftsstelle von Quasi-Niere übermittelt, in der alle wissenschaftlichen und statistischen Analysen zur Qualitätssicherung der Behandlungen erfolgen.

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 nicht anonymisierte Patientenregister beauftragt. Zunächst wurde vom Notar dafür ein Antrag auf notarielle Nebentätigkeit gestellt. Die Präsidentin des Berliner Kammergerichts hat 1996 aber wie folgt beschieden:

„Eine Treuhänderschaft hat den Zweck, die rechtlichen Interessen der Beteiligten zu schützen. Sie stellt damit einen Fall der ‚sonstigen Betreuung der Beteiligten auf dem Gebiete der vorsorgenden Rechtspflege‘ dar; diese aber gehört nach § 24 BNotO zu den Aufgaben der Notare (vgl. auch Seybold-Schippel, BNotO, 6. Aufl., § 24, Rdnr. 7 f, 29). Sie gehört darüber hinaus auch zu den gesetzlichen Aufgaben der Rechtsanwälte nach §§ 1, 3 BRAO (vgl. Feurig-Braun, BRAO, 3. Aufl., § 1 Rdnr. 4, 5, § 3, Rdnr. 5).

Damit stellt die Treuhänderschaft ihrem Wesen nach keine Nebentätigkeit i. S. d. § 8 Abs. 2 BNotO dar, sondern originär notarielle und anwaltliche Tätigkeit, für die es keiner Genehmigung nach § 8 Abs. 2 BNotO bedarf, die der Notar also grundsätzlich ohne weiteres ausüben darf.

Bedenken gegen die Treuhänderschaft unter den Gesichtspunkten des § 14 Abs. 2 BNotO (allgemein mit den Amtspflichten nicht vereinbar, unerlaubte oder unredliche Zwecke) sind nicht erkennbar. Datenschutzrechtliche Gesichtspunkte betreffen die Art und Weise der Durchführung, nicht die grundsätzliche Zulässigkeit der Datentreuhänderschaft. Auf der Hand liegende datenschutzrechtliche Bedenken sind nach der Sachdarstellung des Notars nicht erkennbar; die Abstimmung von Einzelfragen fällt in die Zuständigkeit der Datenschutzbeauftragten, so dass ich hierauf nicht näher eingehe.“

Damit konnte der Einsatz eines Datentreuhänders als vertrauenswürdiger Dritter bei sensiblen Daten realisiert werden.

Im Modellprojekt QuaSi-Niere ist der Datentreuhänder auf Grundlage einer Verfahrensordnung eine selbständige, vertrauenswürdige, eigenverantwortliche und unabhängige Institution. Als eigenständige Daten besitzende Stelle ist er zuständig für die Entgegennahme, Anonymisierung, Deanonymisierung und Weitergabe von 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.

7. Spezielle Fragestellungen einzelner Forschungsgebiete

7.1 Löschungsgebot wider Sicherung guter wissenschaftlicher Praxis

Forschung im idealen Sinne ist Suche nach Wahrheit. Wahrheit ist unlauteren Methoden kategorial entgegengesetzt. Unredlichkeit stellt also die Forschung nicht nur in Frage, sie zerstört sie. Diese Sätze finden sich in den Empfehlungen der Kommission „Selbstkontrolle in der Wissenschaft“ der Deutschen Forschungsgemeinschaft (DFG). Die DFG empfiehlt: „Primärdaten als Grundlage für Veröffentlichungen sollten auf haltbaren und gesicherten Trägern in der Institution, wo sie entstanden sind, für zehn Jahre aufbewahrt werden.“ Entsprechende neue Regelungen finden sich vielfach auch z. B. in Satzungen der Universitäten. Diese Forderung zur Sicherung der Überprüfbarkeit von Forschungsergebnissen durch unabhängige wissenschaftliche Instanzen ist datenschutzrechtlich nicht unproblematisch. Sowohl im Rahmen von Einwilligungserklärungen als auch bei privilegierter Forschung ohne Einwilligung der Betroffenen muss verbindlich dargelegt werden, in welchen Stufen die Einzelangaben anonymisiert oder pseudonymisiert und wann sie vernichtet werden. Die meisten Datenschutzgesetze verlangen eine Löschung der Merkmale, mit denen ein Personenbezug hergestellt werden kann, sobald der Forschungszweck erreicht ist, also spätestens unmittelbar nach Abschluss des Forschungsvorhabens.

Klagen über wissenschaftliches Fehlverhalten hingegen sind voll von Beschreibungen verschwundener Originaldaten und der Umstände, unter denen sie angeblich abhanden gekommen waren. Daraus erwuchs die Forderung, dass es zu den Grundregeln wissenschaftlicher Sorgfalt gehören muss, dass die Originaldaten in der Institution, in der sie entstanden sind, für einen längeren Zeitraum aufzubewahren sind. Um eine Überprüfung im Zusammenhang mit vermutetem Fehlverhalten durch unabhängige wissenschaftliche Gremien zu ermöglichen, ist eine Wiederherstellung des Personenbezuges mitunter erforderlich. Dies steht im Widerspruch zu den Zusicherungen, die den Betroffenen oder den genehmigenden Stellen gegeben werden, dass die Daten „nur im Rahmen dieses Forschungsvorhabens“ verwendet werden. Eine längere Aufbewahrung der Daten und eine Überprüfung der Forschungsergebnisse im Rahmen der Selbstkontrolle der Wissenschaft ist derzeit im Regelfall durch die Formulierung der Einwilligungserklärung bzw. des Antrags auf Übermittlung der Daten (s. 5.) rechtlich nicht abgedeckt. Für dieses Problem müssen noch Lösungen gefunden werden.

Sinnvoll ist jedenfalls, in der Einwilligungserklärung bzw. dem Antrag auf Übermittlung der Daten auf die Verpflichtung der Wissenschaftler zur Einhaltung ihres jeweiligen Ehrenkodexes und die lange Aufbewahrung der Daten zum Zwecke der Überprüfung zu verweisen. Es ist allerdings fraglich, ob die Betroffenen bzw. die Daten besitzende Stelle einer zehnjährigen personenbezogenen Aufbewahrung ihrer Unterlagen und einer evtl. Weitergabe an Prüfer ohne weiteres, insbesondere ohne Einschaltung eines Datentreuhänders, zustimmen. Es sollte geprüft werden, ob der Anonymisierung bzw. der Löschung der Daten ähnlich wirkende organisatorische Möglichkeiten vorgesehen werden können. Die DFG empfiehlt, die Primärdaten nach Abschluss ihrer Auswertung bei einer unabhängigen Stelle zu hinterlegen. Dies käme der Nutzung des Datentreuhänderverfahrens gleich (s. 6.2.4 Archivierungsfunktion des Datentreuhänders). Eine Kombination mit einer Pseudonymisierung und ein Hinterlegen der Pseudonymisierungsalgorithmen in einer dritten Stelle wäre auch ein

angemessenes Verfahren. Dieses hätte – über die Überprüfung der guten wissenschaftlichen Praxis hinaus – den Vorteil, dass unter definierten Umständen und datenschutzgerecht auf alte Primärdaten für spätere Forschungsvorhaben zurückgegriffen werden könnte. Der Datentreuhänder könnte dann als Adressmittler versuchen, mit den Betroffenen in Kontakt zu treten. Wenn er selbst die sensiblen Erhebungsdaten nicht verwahrt, sondern nur über die Hilfsmerkmale verfügt, ist ein solches Verfahren datenschutzrechtlich verantwortbar.

Ergänzend ist zu empfehlen, im Hochschulrecht oder in den Datenschutzgesetzen festzulegen, dass die Übermittlung von personenbezogenen Forschungsdaten durch die Forscher an eine mit Aufsichts- und Kontrollbefugnissen ausgestattete Instanz, die auf Grundlage von Ehrenkodizes tätig wird, im erforderlichen Umfang zulässig ist.

7.2 Neue Probleme bei der Genom-Forschung

Das ursprüngliche Ziel des Human-Genom-Projekts war die Feststellung der Sequenz aller schätzungsweise 3 Milliarden Basenpaare des menschlichen Genoms. Dieses Ziel ist bereits weitgehend erreicht. Die im Rahmen des Projekts untersuchte DNA stammt nicht von einem einzigen Individuum, sondern es wurden überlappende Teile der DNA zahlreicher Menschen verwendet. Die Daten wurden anonymisiert erhoben. Die Untersuchungspersonen haben zur Gewinnung der Daten ihr Einverständnis erteilt. Die künftige genetische Forschung wird sich auf Grundlage der nunmehr vorliegenden Erkenntnisse wesentlich mit der genetischen Konstitution der Menschen beschäftigen. Diese Konstitution kann beispielsweise für die individuelle Auswahl und Dosierung eines Medikaments entscheidend sein. Diese neue Forschungsrichtung wird Pharmacogenomic genannt. Derartige Untersuchungen dürften bald ein fester Bestandteil fast jeder zukünftigen klinischen Studie werden, um unzureichende Wirkung oder unerwünschte Nebenwirkungen von Medikamenten oder anderen Einflüssen auf den Menschen, wie z. B. Umweltbelastungen, zu untersuchen. Derzeit sind auf dem Gebiet der Pharmacogenomic eine Reihe von Firmen- und Forschungsabteilungen, auch in Deutschland, im Entstehen.

Das datenschutzrechtliche Kernproblem dieser Forschung sind, neben der Anonymisierung bzw. Pseudonymisierung der Proben und der Ergebnisse, die Tragweiten der Einwilligung. So liegt die Vermutung nahe, dass es wohl keinen Menschen gibt, der nicht eine genetische Disposition zu einer oder mehreren bestimmten Krankheiten und unterschiedlichen „Verträglichkeiten“ in sich trägt. Generell kann deshalb auch erblich nicht zwischen „gesund“ und „krank“ unterschieden werden. Im Ergebnis der Untersuchung „gesunder“ Probanden werden sich also früher oder später Krankheitsdispositionen herausstellen. Der betroffene Proband kann natürlich frei entscheiden, ob er über diese Dispositionen informiert werden möchte oder nicht. Anders verhält es sich, wenn bereits erkrankte Menschen um ihre Einwilligung in genetische Untersuchungen gebeten werden. Auch diese Forschung ist aus wissenschaftlicher Sicht erforderlich, dass viele genetisch bedingte Erkrankungen, wie z. B. kognitive und psychische Störungen, sich an einem Tier nicht untersuchen lassen, sondern die direkte Einbeziehung von Patienten und deren Familien erfordern. Bereits erkrankte Menschen fühlen sich bekanntlich viel stärker als nicht erkrankte Menschen auch zu einer Teilnahme an einer Forschung verpflichtet, von der sie in keiner Weise mehr profitieren können. Sie sind bereitwilliger, unkritisch auch pauschale Einwilligungen, deren Reichweite (noch) nicht zu übersehen ist, abzugeben. Die Freiwilligkeit ihrer Einwilligung kann aufgrund ihrer Abhängigkeit von der medizinischen Betreuung durch den behandelnden Arzt im Einzelfall in Frage gestellt sein (s. auch 4.3).

Aus diesen Problemstellungen ergibt sich, dass die Forschung, um der Komplexität der Probleme gerecht zu werden und die genetischen Besonderheiten zu untersuchen, auf eine große Zahl von Probanden angewiesen sein dürfte. Ähnlich der isländischen Gendatei ist die Forderung zu erwarten, verschiedenste Daten (genetische Informationen und Proben, Krankheitsgeschichten, Abstammungsangaben) auf eine Person bezogen in Registern zusammenzufassen. Derartige Dateien dürften in der Konsequenz zu Persönlichkeitsprofilen ungeahnter Tiefe einschließlich von möglichen Aussagen über Verwandte führen. Die Datenschutzbeauftragten haben daher – neben Regelungen für genetische Untersuchungen zu medizinischen Zwecken, zur Klärung von Identitäten und Abstammung sowie im Zusammenhang mit Arbeits- und Versicherungsverhältnissen – spezielle Regelungen zur Forschung mit genetischen Daten gefordert und konkrete Vorschläge unterbreitet (Entschließung der 62. Datenschutzkonferenz des Bundes und der Länder vom 24. – 26.10.2001 und Vorschläge zur Sicherung der Selbstbestimmung bei genetischen Untersuchungen).

7.3 Pre-Tests

In der sozialwissenschaftlichen soziologischen und psychologischen Forschung sind Pre-Tests insbesondere bei Fragebogenerhebungen fast selbstverständlich. Hier geht es darum, Schwächen der Fragebögen zu entdecken. Pre-Tests können jedoch aus datenschutzrechtlicher Sicht, insbesondere bei der Bedarfsprüfung, von großer Bedeutung sein. Soll beispielsweise – ohne Einwilligung der Betroffenen oder auch mit deren Einwilligung – auf Datenbestände von Behörden zugegriffen werden, sind diese im Einzelnen den Forschern bei der Beantragung der Genehmigung nicht bekannt. Der Forscher steckt in dem Dilemma, dass er die Art der begehrten personenbezogenen Daten zu benennen hat. Auch eine wirksame Einwilligung setzt voraus, dass die zu nutzenden Daten benannt werden. Genau dieses ist dem Forscher aber, infolge der Unkenntnis der Datenlage vor Beginn der Datenerhebung, faktisch nicht möglich. Er weiß kaum, welche Datenlage er vorfinden wird. Dies gilt insbesondere für Datenbestände, die sich in Akten befinden. Eine Lösung des Problems kann darin liegen, dass den Forschern im Rahmen der Genehmigung die Auflage erteilt wird, das Erhebungsinstrumentarium (beispielsweise den Erhebungsbogen für die aus Akten zu übernehmenden Daten) zunächst anhand einer geringen Zahl von Akten zu testen und erst dann das überarbeitete Erhebungsinstrumentarium vorzulegen. Bei Datenerhebungen mit Einwilligung könnte zunächst eine kleine Anzahl von Betroffenen mit dem Verweis auf die Erprobung der Erhebungsinstrumentarien um ihre Einwilligung gebeten werden. In der anschließenden Hauptphase hat dann die Einwilligungserklärung eindeutig die zu erhebenden Daten und die Forschungsinstrumentarien zu benennen.

7.4 Personen der Zeitgeschichte sowie Funktions- bzw. Amtsträger

Die zeitgeschichtliche Forschung ist oft gefordert, nicht nur auf Daten bundes- oder landesrechtlich verfasster öffentlicher Archive zurückzugreifen. Für Datenbestände, die nach dem Bundesarchivgesetz, den Landesarchivgesetzen oder dem Stasiunterlagengesetz aufbewahrt werden, sind die Möglichkeiten des Zugangs und der Veröffentlichung detailliert geregelt. Für andere Datenbestände, beispielsweise im Justizbereich, musste bis zur Aufnahme einer Forschungsklausel in die Strafprozessordnung ersatzweise auf die allgemeinen Forschungsklauseln der Datenschutzgesetze zurückgegriffen werden. Insbesondere auch bei Forschungsprojekten zur jüngeren deutschen Vergangenheit stellt sich die Frage, ob Personen, die als Amts- oder Funktionsträger tätig waren oder sind, den Schutz des informationellen Selbstbestimmungsrechts in vollem Umfang für sich in Anspruch nehmen können. Zu

beachten ist, dass die Trennlinie zwischen dienstlicher Tätigkeit und persönlichem Status, der eindeutig dem Datenschutz unterliegt, nicht immer klar gezogen werden kann (beispielsweise bei DDR-Unterlagen die „gesellschaftlichen“ Aktivitäten der Beschäftigten und Funktionsträger). Die Grundrechte, einschließlich des Rechts auf informationelle Selbstbestimmung, entfalten ihren Schutz dort, wo die Bürger von staatlicher Gewaltausübung betroffen sind. Soweit Personen hingegen als Amts- oder Funktionsträger in Ausübung hoheitlicher oder fiskalischer Gewalt handeln, können sie sich in ihrer Funktion als Teil der staatlichen Tätigkeit nicht auf die Grundrechte berufen. Die staatliche Tätigkeit als solche steht nicht unter dem Schutz der Grundrechte. Die wissenschaftliche Nutzung oder die anderweitige Einsicht in staatliche Verwaltungsunterlagen einschließlich der Kenntnisnahme der Daten der handelnden Amts- und Funktionsträger bedarf somit keiner besonderen gesetzlichen Grundlage. Auch Amts- und Funktionsträger können sich jedoch auf das Recht auf informationelle Selbstbestimmung berufen, wenn die Verarbeitung der Daten nicht ausschließlich ihre dienstliche Funktion betrifft, sondern sie als Privatperson in ihrem persönlichen Status betroffen sind. Die Abgrenzung ist nicht immer einfach. Im Regelfall ist der Amts- und Funktionsträger durch eine Einsicht Dritter in seine Personalakten als Privatperson betroffen. Deswegen sind Personalakten unter besonderen Geheimhaltungsschutz gestellt. Analysen zur Amtsausübung müssen daher in der Regel ohne Zugriff auf diese Quellen auskommen.

Nicht alle Amts- und Funktionsträger (auch die der ehemaligen DDR) sind von vornherein bezüglich der Nutzung und Veröffentlichung ihrer Daten im Rahmen der zeitgeschichtlichen Forschung mit Personen der Zeitgeschichte gleichzusetzen. Das informationelle Selbstbestimmungsrecht von Personen der Zeitgeschichte tritt nur in dem Maße zurück, wie der eigene Anteil dieser Personen am Ereignis wächst. Wer in der Öffentlichkeit auftritt, dem muss auch die Veröffentlichung der näheren Umstände dieses Wirkens zugemutet werden können. Repräsentanten des Staats, bekannte Sportler oder Schauspieler, aber auch in Anbetracht der deutschen Vergangenheit Personen, die sich schwerer Menschenrechtsverletzungen oder Verbrechen schuldig gemacht haben, können sich also nicht durch den Verweis auf das Recht auf informationelle Selbstbestimmung der Forschung entziehen oder sich einer Veröffentlichung der Ergebnisse im unerlässlichen Rahmen widersetzen. Personen, die sich schwerer Menschenrechtsverletzungen schuldig gemacht haben, können frühestens nach ihrer strafrechtlichen Verfolgung das Recht auf Resozialisierung für sich in Anspruch nehmen, um in der „Anonymität des Vergessens“ zu versinken. Ein Amts- und Funktionsträger hingegen muss hinnehmen, dass seine Mitwirkung an hoheitlichen Maßnahmen (Unterschrift unter einem Bescheid) zum Gegenstand der Forschung gemacht wird und auch veröffentlicht werden darf.

7.5 Zeitweilige Beschäftigung von Forschern bei Daten besitzenden Stellen („One-Dollar-Persons“)

Häufig sind die Daten besitzenden Stellen weder personell noch technisch in der Lage, auch nach einer Genehmigung des Forschungsvorhabens die gewünschten Daten zu selektieren, zu anonymisieren bzw. zu pseudonymisieren oder rechentechnisch aufzubereiten. Eine Lösung für dieses Problem kann es sein, dass für diese Arbeiten ein Auftrag an einen externen Dritten – u. U. auf Kosten des Forschers – vergeben wird (Datenverarbeitung im Auftrag) oder dass Forscher bei der Daten besitzenden Stelle zeitweilig als sog. „One-Dollar-Persons“ beschäftigt werden. Beide Problemlösungen haben allerdings zur Folge, dass Dritte die personenbezogenen Daten der Betroffenen (zeitweilig) zur Kenntnis erhalten. Es ist daher in jedem Fall vorzuzugswürdig, dass die Daten besitzende Stelle diese Arbeiten selbst

durchführt. Wenn dies nicht möglich ist, ist zu prüfen, ob eine Vergabe der Arbeiten an einen externen Dritten vorzuziehen ist, der kein inhaltliches Interesse an den Daten hat. Dieser Weg wird allerdings vielfach wegen der Komplexität der Arbeiten, des eingeschränkten Fachwissens der Auftragnehmer, der dort anfallenden Datenschutzprobleme und der auftretenden Kosten nicht gangbar sei.

Als sog. „One-Dollar-Persons“ werden in den USA Forscher zeitweilig und unentgeltlich oder gegen ein symbolisches Entgelt bei den Daten besitzenden Stellen angestellt, um diese wissenschaftlichen Vorarbeiten zu erledigen. Auch das deutsche Datenschutzrecht steht (ohne eine abschließende Prüfung der arbeits- und versicherungsrechtlichen Fragen) unter bestimmten Voraussetzungen im Einzelfall dieser Möglichkeit grundsätzlich nicht entgegen, sofern keine Umgehungstatbestände geschaffen und dieselben Geheimhaltungsregeln wie bei vollbeschäftigten Forschern eingehalten werden.

Die Datenverwendung von Forschern im Rahmen eines „One-Dollar-Anstellungsverhältnisses“ beinhaltet in der Regel drei Phasen:

- Kenntnisnahme und Selektion der Daten,
- Anonymisierung bzw. Pseudonymisierung der zu verarbeitenden Daten,
- weitere Verwendung der anonymisierten oder pseudonymisierten Daten für die Forschungsarbeiten.

Das datenschutzrechtliche Problem liegt hier in der ersten Stufe, der Kenntnisnahme der Daten durch den Forscher. Diese hat eine rechtliche Doppelnatur. Zum einen ist sie Datenverarbeitung in Form der Datennutzung für die den Forscher anstellende Stelle (beispielsweise zur Erfüllung der Anonymisierungsverpflichtungen), zum anderen ist sie bereits Datennutzung zu Forschungszwecken im Interesse des Forschenden. Rechtlich unterliegt dieser Teil der Tätigkeit den Forschungsklauseln der speziellen Rechtsvorschriften bzw. der Datenschutzgesetze. Die Zweckbindung ist dabei auf das jeweilige einzelne Forschungsprojekt abgestellt. Bei einem so angestellten Forscher liegt dann eine „Eigenforschung“ nach § 30 Abs. 6 BlnDSG oder § 33 Abs. 1 HDSG vor.

Das privatrechtliche Anstellungsverhältnis des Forschers ist zivilrechtlich dann unwirksam, wenn es sich um ein Scheingeschäft (§ 117 BGB) handelt. Dies ist jedoch nicht der Fall, wenn die mit den Forschern abgeschlossenen Verträge gerade eine wirksame Rechtsgrundlage für deren Tätigkeit bezwecken. Es wird dann gerade nicht der Schein von Rechts-erklärungen geschaffen, die so nicht wirksam werden sollen. Es wird kein „normales“ Arbeitsverhältnis vorgetäuscht. Ein solches Beschäftigungsverhältnis ist dann nichtig, wenn es auf die Umgehung datenschutzrechtlicher Vorschriften abzielt, etwa eine Aushöhlung von rechtlichen Hürden der Forschung bezweckt. Ihr Ziel liegt nicht in der Umgehung von Hürden, sondern in der Sicherung der datenschutzrechtlichen Erfordernisse. Sie sichern die Verpflichtung des Forschers zur Geheimhaltung und die Modalitäten des Datenzugangs vertraglich und vermeiden, dass durch die Kenntnisnahme der personenbezogenen Daten durch die Forschung für die Betroffenen von der gesetzlichen Regelung ausgeschlossene Risiken entstehen. Sie dienen damit einer Ausgestaltung des Verhältnisses von Forscher und Daten besitzender Stelle im Rahmen der datenschutzrechtlichen Vorgaben. Vertragsgestaltungen, die etwa verbleibende „Gesetzeslücken“ auszunutzen suchen und damit eine Umgehung der datenschutzrechtlichen Vorschriften bezwecken, sind zivilrechtlich unwirksam, weil sie das Verbot des Umgehungsgeschäfts gemäß § 134 BGB verletzen. Datenschutzrechtlich fehlt dann eine Legitimation zur Kenntnisnahme der personenbezogenen Daten durch den Forscher.

7.5.1 One-Dollar-Person und das Statistikgeheimnis

Die Vorschriften zur Wahrung des Statistikgeheimnisses bei der Übermittlung von Einzelangaben an Forschungseinrichtungen (§ 16 Abs. 6 BStatG) legen fest, dass vor der Übermittlung eine faktische Anonymisierung der Daten vorzunehmen ist. Die Anonymisierung ist damit Aufgabe der statistischen Ämter. Im Einzelfall kann es wegen fehlender personeller und finanzieller Ressourcen der statistischen Ämter vertretbar sein, dass die Anonymisierung vom angestellten Forscher erledigt wird. Der Forscher als Bediensteter des statistischen Amtes unterliegt den strafbewehrten Bestimmungen des Statistikgeheimnisses. Des Weiteren kann durch seine Anonymisierungsarbeiten im Amt erreicht werden, dass die bloße faktische Anonymisierung nach § 16 Abs. 6 BStatG durch den gesteigerten Anonymisierungsgrad des § 16 Abs. 1 Nr. 4 BStatG ersetzt und damit auch die Möglichkeit der Weitergabe und Veröffentlichung durch den Forscher nach Beendigung seines Anstellungsverhältnisses im statistischen Amt eröffnet wird.

7.5.2 Ärzte als One-Dollar-Persons und die ärztliche Schweigepflicht

Die ärztliche Schweigepflicht ist so restriktiv, dass eine Übermittlung von Patientendaten nur erlaubt ist, wenn die Anonymität des Patienten gesichert ist oder dieser ausdrücklich eingewilligt hat. Da die ärztliche Schweigepflicht als Standesrecht der Ärzte allein an die berufliche Eigenschaft als Arzt anknüpft, gilt sie unabhängig von den zusätzlichen „Rollen“, die der Arzt gleichzeitig innehat. Die Schweigepflicht besteht also für den Arzt unabhängig davon, in welcher Form sein Anstellungsverhältnis vorgenommen wurde. Damit sind auch für forschende Ärzte „One-Dollar-Person“-Verträge zulässig.

7.6 Erweiterter Zugang von Forschern zu Daten der amtlichen Statistik

Die Art der Nutzung statistischer Daten hat sich in der Informationsgesellschaft verändert. Wirtschaftlicher und sozialer Wandel kann nur untersucht werden, wenn Informationen auf der Mikroebene von Beobachtungseinheiten (Personen, Haushalte, Unternehmen) zu verschiedenen Zeitpunkten für statistische Zwecke verfügbar und zugänglich sind. Moderne statistische Methoden erfordern den Zugang zu Mikrodaten, um Verhaltensregelmäßigkeiten und -zusammenhänge aufzudecken.

Die Bundesministerin für Bildung und Forschung hat daher eine Kommission gebeten zu klären, ob die informationelle Infrastruktur der Bundesrepublik Deutschland dieser veränderten Aufgabenstellung noch gerecht wird, und sie beauftragt, Vorschläge zur Verbesserung der informationellen Infrastruktur zwischen Wissenschaft und Statistik zu erarbeiten. Der Auftrag der Kommission zielte auf die generelle Verbesserung der Kooperation zwischen Statistik und Wissenschaft. Er schloss alle Datenquellen ein.

Das Gutachten der Kommission enthält zahlreiche Empfehlungen zur Verbesserung des Umgangs von Forschern zu Daten der amtlichen Statistik. Zur Sicherstellung des Datenschutzes empfiehlt es die Einführung eines Forschungsdatengeheimnisses, das auch ein Zeugnisverweigerungsrecht des Wissenschaftlers im Hinblick auf Forschungsakten und ein entsprechendes Beschlagnahmeverbot enthält.

8. Forschungsregister

Auch die wissenschaftlich begründete Registrierung eines Menschen in Form der langfristigen Speicherung seiner personenbezogenen Daten stellt einen Eingriff in sein Persönlichkeitsrecht dar. Wissenschaftliche Daten werden nicht selten auf Vorrat gehalten. Der Betroffene vermag die Auswirkungen auf sein Leben im Vorhinein meist nicht zu übersehen. Die Europäische Datenschutzrichtlinie hebt aus der Gesamtheit der zu schützenden personenbezogenen Daten Daten über Rasse, politische Meinung, Religion, Gewerkschaft, Gesundheit und Sexualverhalten als sensitiv und besonders schutzwürdig hervor. Soweit in Forschungsregistern sensitive Daten (beispielsweise über Erkrankungen) personenbezogen vorgehalten und u. U. an Dritte weitergegeben werden sollen, wird im Regelfall nicht nur eine spezialgesetzliche Grundlage für die Führung des Registers gefordert werden müssen. Zusätzlich müssen besondere Rechtfertigungsgründe gegeben werden, wenn derartige Daten unverschlüsselt verarbeitet werden sollen, statt anonymisiert oder pseudonymisiert zu werden. Der Aufbau personenbezogener Register ausschließlich auf der Grundlage einer Einwilligung der Betroffenen ist nicht datenschutzgerecht, weil für die Betroffenen nicht übersehbar ist, wer welche Daten wann und wo für welche Zwecke verwenden wird. Die Modalitäten der Verfahrensweise können vom Einzelnen nicht gesteuert werden. Außerdem sind die im Zusammenhang mit dem Aufbau eines solchen Registers zu klärenden datenschutzrechtlichen Fragen so komplex, dass sie einer klaren und auch langfristig verbindlichen Festlegung bedürfen. Ein Beispiel hierfür sind die Landeskrebsregistergesetze, die insbesondere die Fragen der rechtlichen Voraussetzungen einer Meldung an das Register, Umfang und Ausgestaltung des Registers, Voraussetzungen einer Datenübermittlung an Forscher, Durchführung von Datenabgleichen etc. detailliert regeln.

Werden die Daten im Register anonymisiert oder pseudonymisiert gespeichert und werden weitere Verfahrensvorschriften festgelegt, die eine Reidentifizierung verhindern, sind spezialgesetzliche Regelungen verzichtbar.

Häufig wollen die Forscher einen begrenzten Personenbezug erhalten, um neue Einzeldaten der Betroffenen mit den vorhandenen Registerdaten zu verbinden. Dafür bieten sich Pseudonymisierungsverfahren an, die mit Hilfe eines Datentreuhänders in der Rolle eines vertrauenswürdigen Dritten durchgeführt werden können. Wenn der Betroffene bei einem derartigen Verfahren hinreichend transparent informiert wird und er deutlich auf seine Widerspruchsmöglichkeiten hingewiesen wird, ist seine Einwilligung auch bei dieser Form der Registerspeicherungen rechtswirksam, solange die Modalitäten der Verwendung der Daten für ihn übersehbar sind. Diese Verfahren sichern auch die Beschlagnahmefestigkeit der Daten des Registers, da dann nur pseudonymisierte Daten gespeichert sind. Für den Datentreuhänder sollte ein Zeugnisverweigerungsrecht bestehen (Anwalts-, Notarmodell s. 6.2.1).

Das grundsätzliche Problem liegt auch bei Registern mit pseudonymisierten Daten darin, dass von einer strikten Zweckbindung (vergleichbar der amtlichen Statistik) nicht gesprochen werden kann. Für die amtliche Statistik bezeichnete das Bundesverfassungsgericht in seinem Volkszählungsurteil die Geheimhaltung der personenbezogenen Einzeldaten als

konstitutionell. Genau dies ist aber bei einer Registerforschung oft nicht möglich. Unter Umständen müssen den Forschern personenbezogene Einzeldatensätze zur Auswertung zugänglich gemacht werden. Ferner bedarf die Forschungsrichtung aufgrund neuer wissenschaftlicher Erkenntnisse häufig einer Änderung.

Selbst ein in einem Register gespeicherter pseudonymisierter Einzeldatensatz kann ein erhebliches Reidentifizierungspotenzial in sich bergen, wenn dieser eindeutige Regionalangaben (beispielsweise die fünfstellige Postleitzahl) und seltene Merkmalskombinationen enthält. Daher sollten vor einer Einspeicherung von Daten in ein Forschungsregister regionale Bezüge und auch andere Merkmale wie beispielsweise das komplette Geburtsdatum umkodiert und stattdessen nur Gruppen mit weniger Merkmalsausprägungen verwendet werden. Dies reduziert die Bestimmbarkeit der Personen und erhöht den Grad ihrer Anonymisierung.

Weiterführende Literatur

-
- Bizer, Johannes: Der Datentreuhänder. DuD 1999, 392
 - Bizer, Johannes: Forschungsfreiheit und Informationelle Selbstbestimmung, Nomos Universitätsschriften. Baden-Baden: Nomos Verlagsgesellschaft, 1992
 - Informationsblatt Datenschutz und Forschung. Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern, Schloss Schwerin, 19053 Schwerin
 - Wissenschaftliche Forschung: Informationen zum Datenschutz Heft 3. Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz, Deutschhausplatz 12, 55116 Mainz, <http://www.datenschutz.rlp.de>
 - Deutsche Arbeitsgemeinschaft für Epidemiologie (DAE)/Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Epidemiologie und Datenschutz 1998. Der Hessische Datenschutzbeauftragte, Uhlandstraße 4, 65189 Wiesbaden, <http://www.hessen.de/hdsb>
 - Empfehlungen der Kommission „Selbstkontrolle in der Wissenschaft“: Vorschläge zur Sicherung guter wissenschaftlicher Praxis. Deutsche Forschungsgemeinschaft, Januar 1998, <http://www.dfg.de>
 - Selbstbestimmung und Erkenntnisdrang, 1998. Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Postfach 20 04 44, 40102 Düsseldorf, <http://www.lfd.nrw.de>
 - Fröhlich, Uwe: Forschung wider Willen? Berlin/Heidelberg: Springer-Verlag, 1999
 - Gerling, Rainer W.: Datenschutzprobleme in der Forschung. DuD 1999, 384
 - Hamm, Rainer; Möller, Klaus (Hrsg.): Datenschutz und Forschung, Forum Datenschutz Bd. 7. Baden-Baden: Nomos Verlagsgesellschaft, 1999
 - Hauser, Richard; Wagner, Gert G.; Zimmermann, Klaus: Erfolgsbedingungen empirischer Wirtschaftsforschung und empirisch gestützter wirtschafts- und sozialpolitischer Beratung: Ein Memorandum. Allgemeines Statistisches Archiv 82 (1998), 369-379
 - Jehle, Jörg-Martin (Hrsg.): Datenschutz und Datenzugang in der Kriminologischen Forschung, Kriminologie und Praxis Bd. 2. Wiesbaden: Kriminologische Zentralstelle e.V., 1987
 - Kommission zur Verbesserung der informationellen Infrastruktur zwischen Wissenschaft und Statistik: Wege zu einer besseren informationellen Infrastruktur. Baden-Baden: Nomos Verlagsgesellschaft, 2001
 - Lercher, Thomas: Datenschutz und psychologische Forschung. Göttingen: Verlag für Psychologie Dr. C. J. Hogrefe, 1988
 - Medizinisches Forschungsgeheimnis: Resolution der Arbeitsgemeinschaft der Wissenschaftlichen Medizinischen Fachgesellschaften (AWMF) vom 9. Mai 1998. DuD 1999, 413

- Metschke, Rainer; Wellbrock, Rita: Statistikgeheimnis und Datenschutz wider die empirische (Wirtschafts-)Forschung? Anmerkungen zum Memorandum. Allgemeines Statistisches Archiv 83 (1999), 152
- Schulte, Jörg; Wehrmann, Rüdiger; Wellbrock, Rita: Das Datenschutzkonzept des Kompetenznetzes Parkinson. DuD 2002, 605
- Simitis, Spiros: Datenschutz – Ende der medizinischen Forschung? MedR 1985, 195
- Simitis, Spiros: Programmierter Gedächtnisverlust oder reflektiertes Bewahren: Zum Verhältnis von Datenschutz und historischer Forschung. Festschrift Zeidler, 1987, 1475 ff.
- Überla, Karl; Zeiler, Joachim (Hrsg.): Datenschutz und Wissenschaftsadministration im Gesundheitsbereich. BGA-Schriften 3/83. München: MMV Medizin Verlag
- Vetter, Rainer: Forschungs(daten)geheimnis. DuD 1999, 389
- Wagner, Gert: Wissenschaft schützt die Öffentlichkeit vor schlechten statistischen Ergebnissen. DuD 1999, 377.

In der Schriftenreihe „Materialien zum Datenschutz“, unter der auch diese Broschüre erscheint, bietet der Berliner Beauftragte für Datenschutz und Informationsfreiheit u. a. das „Volkszählungsurteil“ vom 15. Dezember 1983 Interessenten kostenlos an (Materialien Heft 1).

Anlage 1 – Beispiele für Einwilligungserklärungen

1. Im Folgenden möchten wir Sie über die Einzelheiten des von uns geplanten Forschungsvorhabens informieren:

Verantwortlicher Träger und Leiter des Forschungsvorhabens

...

Zweck des Forschungsvorhabens

...

Umgang und Art und Weise der Datenverarbeitung (Inhalt der Datensätze, Verarbeitung der Daten in anonymisierter, pseudonymisierter oder personenbezogener Form, Ort der Verarbeitung der Daten, ggf. Einsatz eines Treuhänders usw.)

...

Personenkreis, der von personenbezogenen Daten Kenntnis erhält (Mitarbeiter des Forschungsinstituts oder ausschließlich der Treuhänder, evtl. Empfänger der Daten oder Abrufberechtigte, evtl. Auftragsdatenverarbeitung)

...

In die Studie einbezogene Kooperationspartner, soweit sie mit eigenständigen Aufgaben bei der Verarbeitung personenbezogener Daten bekannt sind (z.B. beteiligtes Forschungsinstitut)

...

Ihre personenbezogenen Daten werden nur für dieses Forschungsvorhaben verwendet. Sie werden nicht an Dritte zu anderen Zwecken weitergegeben, es sei denn, Sie willigen erneut in einer späteren Einwilligungserklärung in eine solche Weiterübermittlung der Daten ein.

2. Sobald der Forschungszweck dies erlaubt, werden die Informationen, mit denen ein Personenbezug hergestellt werden kann, aus Datensicherheitsgründen gesondert gespeichert.
3. Sobald der Forschungszweck es zulässt, werden Ihre personenbezogenen Daten vernichtet bzw. gelöscht. Dies wird spätestens am ... sein.
4. Ihre Einwilligung ist freiwillig. Durch eine Verweigerung der Einwilligung entstehen Ihnen keine Nachteile. Sie können Ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen und die Löschung bzw. Vernichtung Ihrer Daten verlangen.
5. Ich habe die Information über das Forschungsvorhaben erhalten. Ich bin mit der vorgesehenen Verarbeitung meiner Daten einverstanden.

.....
Ort, Datum

.....
Unterschrift

Beispiel 1

Kopfbogen der Forschungseinrichtung

mit Anschrift

Name des Projektleiters

Telefon-/Faxnummer

Berlin, 200__

Liebe Eltern,

wie Sie vielleicht wissen, nimmt die Klasse Ihres Kindes seit Mitte 1994 an dem Projekt, das unter meiner Leitung steht, teil.

Unsere Längsschnittstudie bezieht Schülerinnen und Schüler aus 30 Berliner Grundschulklassen ein und erfragt von der 2. Klasse an die Entwicklung der Schul.....

Im Sommer des letzten Jahres wechselten die in unserer Studie einbezogenen Kinder in eine weiterführende Schule. Neue Lehrer und Mitschüler, neue Unterrichtsfächer und Lernanforderungen sind zu verkraften. Uns interessiert deshalb die Frage, wie

Es gibt kaum Längsschnittstudien, die Schulleistungen und sowie familiäre und schulische Kontextbedingungen über einen längeren Zeitraum beginnend in der Grundschule bis in die Sekundarstufe I erfassen. Um so erfreulicher ist es, dass wir fast 300 Schülerinnen und Schüler zu unserer Längsschnittstichprobe zählen können, die wir seit 1994 jährlich befragen. Unser Ziel ist es, möglichst viele Schülerinnen und Schüler in ihren weiterführenden Schulen wiederzufinden und weiterhin zu befragen.

Diese Befragung soll im Zeitraum Februar – März 200__ innerhalb der Schulklassen erfolgen, in denen die Kinder unserer Längsschnittstudie unterrichtet werden. Die Beantwortung des Fragebogens wird nicht länger als eine Unterrichtsstunde dauern.

Die Anonymität der Befragung wird wie bisher dadurch gewährleistet, dass die Schülerinnen und Schüler ihre Namen selbst codieren. Eine Liste der Zuordnungen von Namen und Codeworten wird notariell hinterlegt und dient nur der Kontaktaufnahme bei möglichem Schulwechsel. Unsere Untersuchung ist von der Senatsverwaltung für Schule genehmigt worden und berücksichtigt die Hinweise des Berliner Beauftragten für Datenschutz und Informationsfreiheit.

Da Längsschnittstudien, die über einen so langen Zeitraum die schulische Entwicklung von Schülerinnen und Schülern erfassen, überaus schwierig und selten sind, haben wir ein sehr großes Interesse an jedem einzelnen Kind. Deshalb bitten wir Sie sehr, Ihre Zustimmung zu geben, dass Ihr Kind an der Befragung teilnehmen kann. Falls Ihr Kind noch nicht an einer unserer Befragungen teilgenommen hat, bitten wir Sie ebenfalls um Ihre Zustimmung.

Wenn Sie einverstanden sind, dass Ihr Kind an der Befragung teilnimmt, unterschreiben Sie bitte die Einverständniserklärung und geben Sie diese an die Schule zurück. Die Einverständniserklärungen werden in der Schule aufbewahrt und nach Abschluss der Befragung vernichtet. Die Schule sichert, dass nur Schüler an der Befragung teilnehmen, für die die Einwilligung der Eltern vorliegt. Selbstverständlich ist die Teilnahme an der Befragung freiwillig. Es entstehen Ihnen keine Nachteile, wenn Sie nicht teilnehmen. Auch können Sie jederzeit – solange die erhobenen Daten durch die Codierung noch personenbeziehbar sind – Ihre Einwilligung widerrufen und die Löschung der Daten Ihres Kindes von uns verlangen.

Mit freundlichen Grüßen und auf Ihre Mitarbeit hoffend

Prof. Dr.
(Projektleiter/in)

Einverständniserklärung

Hiermit erkläre ich mein Einverständnis, dass mein Kind an der Befragung zur Fortsetzung des Projektes teilnimmt.

.....
Ort, Datum

.....
Unterschrift

Beispiel 2

Erklärung zum Datenschutz und zur absoluten Vertraulichkeit Ihrer Angaben

Das Institut für ist ein Institut des Unsere Arbeit folgt streng den Bestimmungen des Datenschutzes. Die Weitergabe persönlicher Daten an Dritte ist daher nicht möglich. Die erbetenen Angaben unterliegen der ärztlichen Schweigepflicht und werden unter Wahrung der datenschutzrechtlichen Bestimmungen wissenschaftlich ausgewertet.

Name, Anschrift und Telefonnummer stehen nur auf der Einverständniserklärung. Dies gibt uns die Möglichkeit, Ihnen ggf. auffällige Befunde bei der mitzuteilen. Die Einverständniserklärung wird getrennt aufbewahrt; die darin enthaltenen persönlichen Angaben werden nicht gespeichert. Nach Studienende (Ende 200_) wird die Einverständniserklärung vernichtet. Eine Zuordnung der erhobenen Daten zu einer bestimmten Person ist dann nicht mehr möglich.

Was geschieht mit Ihren Angaben im Fragebogen und den medizinischen Messwerten?

Unsere Mitarbeiter wandeln die Fragebogendaten (Kreuze und Nennungen) in statistische Zahlen um und geben diese Zahlen ohne Ihren Namen oder Ihre Adresse in den Computer ein. Die medizinischen Messergebnisse und die Angaben aus dem Fragebogen werden nur durch eine Codenummer miteinander verknüpft. Eine Verbindung von Codenummer mit Ihrem Namen und Adresse ist nach Abtrennung der Code-Nummer von der Einverständniserklärung (Mai 200_) nicht mehr möglich. Die Ergebnisse der medizinischen Untersuchung und Befragung werden ausschließlich in anonymisierter Form und für Gruppen zusammen dargestellt. Das bedeutet, niemand kann später aus den Ergebnissen erkennen, von welcher Person die Angaben gemacht worden sind bzw. welcher medizinische Messwert zu welcher Person gehört.

Sollten Ihrerseits Fragen hinsichtlich des Datenschutzes bestehen, können Sie sich jederzeit auch an den Berliner Beauftragten für Datenschutz und Informationsfreiheit wenden (Tel.: 75 60–78 09, Vorgang), dessen Hinweise wir berücksichtigen haben.

Prof. Dr.
(Projektleiter/in)

Informationsschreiben

Kopfbogen

Liebe Frau,

Sie haben, wie Sie sich sicherlich erinnern werden, Ende 1997 an der Befragung im Rahmen unseres Forschungsprojektes „Soziopsychosomatisch orientierte Begleitung in der“ teilgenommen. Für Ihre bisherige Mitarbeit danken wir sehr. Sie hatten uns damals Ihr Einverständnis gegeben, Sie für eine Nachfolgeuntersuchung nochmals anschreiben zu dürfen.

Nunmehr wenden wir uns an Sie mit der Bitte um Unterstützung für eine vom Bundesministerium für Forschung und Technologie geförderte Nachfolgeuntersuchung mit dem Schwerpunkt Die von Ihnen hinsichtlich verschiedener Lebensbereiche gemachten Angaben sollen bei dieser neuen Untersuchung in Verbindung mit den medizinischen Dokumentationen dazu beitragen, näheren Aufschluss über die Auswirkungen biologischer, seelischer und sozialer Faktoren auf den zu erhalten. Dadurch wird es möglich sein, entsprechende Risiken zu benennen und adäquate vorbeugende Maßnahmen zur Verhinderung von Komplikationen anzubieten.

Sollten Sie Ihrerseits Fragen zum Verlauf der Untersuchung haben, können Sie sich gern an unsere Mitarbeiterinnen, Tel., wenden. Auf Wunsch informieren wir Sie nach Abschluss des Projektes auch über Ergebnisse der Untersuchung.

Ihre Einwilligung ist selbstverständlich wieder freiwillig. Aus der Ablehnung Ihrer weiteren Mitarbeit entstehen Ihnen keine Nachteile.

Sie können Ihre Einwilligung mit Wirkung für die Zukunft jederzeit widerrufen und eine Löschung Ihrer Daten verlangen.

Prof. Dr.
(Projektleiter/in)

Einverständniserklärung

Ich erkläre mich einverstanden, an der Befragung im Rahmen des Forschungsprojektes
„Soziopsychosomatisch orientierte Begleitung in der“
teilzunehmen.

Darüber hinaus erteile ich die Genehmigung zur Einsicht in meine Unterlagen. Der
Datenschutz muss entsprechend der beigefügten „Erklärung zum Datenschutz und zur abso-
luten Vertraulichkeit Ihrer Angaben“ gewährleistet sein.

Die Einverständniserklärung wird nach Abschluss des Projektes (voraussichtlich Ende
200_) vernichtet.

.....
Ort, Datum

.....
Unterschrift

(wird nach Einsicht in die Unterlagen abgetrennt und vernichtet)

Name, Vorname

--

Anschrift (1997)

--

Geburtsdatum

--	--	--

Tag

Monat

Jahr

Fragebogennummer

(Bitte nicht ausfüllen)

Die aus den Unterlagen übernommenen Daten werden nur unter der Fragebogen-
nummer gespeichert. Der Name, die Anschrift von 1997 und das Geburtsdatum benötigen
wir nur zum Auffinden Ihrer Unterlagen und zur Dokumentation Ihrer Einwilligung gegen-
über, die Ihre Unterlagen archiviert hat.

Beispiel 3

**Einverständniserklärung
des Patienten zur Übermittlung seiner Daten
an das Projekt QuaSi-Niere**

Die Informationsbroschüre des Projektes QuaSi-Niere und die Rückseite dieses Blattes habe ich gelesen. Zusätzliche Fragen zu dem Projekt und den Vorkehrungen zum Schutz der persönlichen Daten wurden mir durch meinen Arzt beantwortet.

Ich bin davon unterrichtet worden, dass die Teilnahme an dem Projekt freiwillig ist und mir keine Nachteile aus einer Nichtteilnahme entstehen.

Ich ermächtige hiermit meinen behandelnden Arzt, medizinische Daten meiner Nierenerkrankung, der Miterkrankungen und die Umstände meiner Behandlung (bzw. die Daten meines nicht volljährigen Kindes) über die Vertrauensstelle an die Projektgeschäftsstelle QuaSi-Niere in Berlin weiterzuleiten.

Als Dokument der Bereitschaft zur Teilnahme wird ein QuaSi-Niere-Ausweis (Chipkarte) mit dem Namen, Vornamen, Geburtsdatum, Geschlecht und einer Patientennummer ausgestellt. Durch die Vorlage dieses Ausweises ermächtige ich auch weitere behandelnde Ärzte, medizinische Informationen an das Projekt QuaSi-Niere weiterzuleiten.

Persönliche Daten Ich erlaube mir die namentliche Übermittlung meiner Daten an die Vertrauensstelle (die Daten werden in der Vertrauensstelle anonymisiert) und wünsche keine direkte Anonymisierung.

Falls vorhanden und möglich

EDTA-Nummer* Ich gebe mein Einverständnis zur Übermittlung meiner EDTA-Nummer.

Eurotransplantnummer Ich gebe mein Einverständnis zur Übermittlung meiner Anmelde-nummer bei Eurotransplant (ET-Nummer).

*** Bitte streichen Sie die Absätze durch, wenn kein Einverständnis gegeben wird.**

Die EDTA-Nummer und die ET-Nummer werden bei der Vertrauensstelle gespeichert und sollen der Zusammenführung von Behandlungsinformationen aus verschiedenen Registern dienen. Diese Zahlen erleichtern Ihren behandelnden Ärzten die Arbeit der regelmäßigen Übermittlung der Informationen.

Diese Einverständniserklärung kann jederzeit widerrufen werden.

.....
Ort, Datum

.....
Unterschrift/en

(Bei Minderjährigen reicht die Einwilligung der Sorgeberechtigten nicht aus. Bei Einsichtsfähigkeit hat der Minderjährige sein Einverständnis zusätzlich auch zu geben.)

Diese Einverständniserklärung verbleibt beim behandelnden Arzt.

***Erläuterungen
für die Erteilung der Einverständniserklärung***

Der Patient erteilt umseitige Einverständniserklärung zur Erhebung und Verarbeitung von Behandlungsinformationen.

Diese Einverständniserklärung wird unter der Voraussetzung gegeben, dass

- ❶ diese Daten vom behandelnden Arzt ausschließlich an eine hierfür eingerichtete, vertrauenswürdige Daten besitzende Stelle (Datentreuhänder als Vertrauensstelle des Projektes QuaSi-Niere) weitergeleitet werden,
- ❷ die Vertrauensstelle der ihr auferlegten Verpflichtung nachkommt, die Daten unverzüglich zu verarbeiten, und dabei die Daten zur Person des Patienten so verschlüsselt werden, dass eine Verbindung und Rückführung der Daten durch Dritte zu diesem Patienten ausgeschlossen ist. Nach Eingabe und Verschlüsselung der Angaben zur Person werden diese von den Fragebögen getrennt und vernichtet. Eine Rückführung und Verbindung zur Person ist nur möglich durch Anforderung des behandelnden Arztes oder durch Anforderung des Patienten bei der Vertrauensstelle mit Angabe eines Arztes, an den die Daten geschickt werden sollen,
- ❸ eine Chipkarte mit dem Namen, Vornamen, Geburtsdatum, den Seriennummern der Chipkarte und einer willkürlichen, aber eindeutigen Patientennummer erstellt wird (diese Patientennummer ist nicht die Ordnungsnummer der Datensätze in der Projektgeschäftsstelle QuaSi-Niere),
- ❹ nur verschlüsselte Daten zur weiteren Auswertung von der Vertrauensstelle an die Projektgeschäftsstelle QuaSi-Niere und zurück geleitet werden,
- ❺ alle von ihm erlangten Daten auf jederzeit mögliches Verlangen des Patienten so vollständig verschlüsselt werden, dass eine Verbindung und Rückführung zu ihm endgültig ausgeschlossen ist.

Anlage 2 – Beispiele für Codierungen

Beispiel 1

Geschl.	Geburtsdatum	Nachname

1 = m 2 = w	JJ	MM	2. od. 3.*	letzter	Anzahl	
Geschl.	Geb.-Jahr	Geb.-Monat	Buchstaben des Nachnamens			

Hinweise zur Bearbeitung des Codierbogens:

- Vom Geburtsdatum sollen das Jahr und der Monat zweistellig, im Bedarfsfall mit führender Null, übernommen werden.
- Wenn die Anzahl der Buchstaben des Nachnamens mehr als neun (9!) beträgt, ist eine Null (0!) einzutragen.
- Umlaute (ä, ü, ö) werden als zwei Buchstaben geschrieben (a = ae; ö = oe; ü = ue).
- Bei zusammengesetzten Familiennamen wird nur der erste Namensteil berücksichtigt.
- Namenszusätze wie beispielsweise „Dr.“, „Baron von“ oder „von“ entfallen.
- ß bleibt als Buchstabe unverändert.

- * Beim 3. Buchstaben des Vor- oder Nachnamens wird eine bessere Gleichverteilung der Möglichkeiten erreicht.

Beispiel 2

Um deine Antwort richtig zuordnen zu können, ohne die Geheimhaltung zu verletzen, benötigst du der Fragebogen ein Kennwort.

Das Kennwort ist wie folgt aufgebaut:

1. die beiden ersten Buchstaben des Vornamens deiner Mutter
2. dein eigener Geburtstag
3. die beiden ersten Buchstaben des Vornamens deines Vaters

Beispiel:

Vorname der Mutter: **Elke** ☐ ☐

eigener Geburtstag: **09.11.1987** ☐ ☐

Vorname des Vaters: **Helmut** ☐ ☐

Daraus ergibt sich das Kennwort: **EL 09 HE**

Wenn du den jeweiligen Vornamen von Vater oder Mutter nicht kennst, schreibe statt der jeweiligen Anfangsbuchstaben XX.

Bitte trage jetzt in die Kästchen dein Kennwort ein:

Die beiden ersten Buchstaben des Vornamens deiner Mutter: ☐ ☐

Dein eigener Geburtstag (nur der Tag): ☐ ☐

Die beiden ersten Buchstaben des Vornamens deines Vaters: ☐ ☐

Bemerkung:

Die Nutzung des 2. und 3. Buchstabens lässt die Anzahl gleicher Paare bei unterschiedlichen Personen deutlich sinken. Es ist auch eine Kombination aus den jeweils 3. Buchstaben von Vor- und Nachnamen, gepaart jeweils mit der Anzahl der Buchstaben des Namens oder dem Geburtstag günstig.

Das Deanonymisierungspotenzial wird deutlich gesenkt, wenn statt des eigenen Nachnamens der Geburtsname der Mutter genutzt wird.

Anlage 3 – Auszüge der in dieser Broschüre eingehend dargestellten Regelungen

3.1 Bundesrecht

3.1.1 Grundgesetz der Bundesrepublik Deutschland

Art. 1 Schutz der Menschenwürde

- (1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.
- (2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.
- (3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

Art. 2 Allgemeines Persönlichkeitsrecht

- (1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.
- (2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

Art. 5 Meinungsfreiheit

- (1) Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.
- (2) Diese Rechte finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre.
- (3) Kunst und Wissenschaft, Forschung und Lehre sind frei. Die Freiheit der Lehre entbindet nicht von der Treue zur Verfassung.

Art. 6 Ehe und Familie, nicht eheliche Kinder

- (1) Ehe und Familie stehen unter dem besonderen Schutze der staatlichen Ordnung.
- (2) Pflege und Erziehung der Kinder sind das natürliche Recht der Eltern und die zuvörderst ihnen obliegende Pflicht. Über ihre Betätigung wacht die staatliche Gesellschaft.

Art. 79 Änderung des Grundgesetzes

(3) Eine Änderung dieses Grundgesetzes, durch welche die Gliederung des Bundes in Länder, die grundsätzliche Mitwirkung der Länder bei der Gesetzgebung oder die in den Artikeln 1 und 20 niedergelegten Grundsätze berührt werden, ist unzulässig.

3.1.2 Volkszählungsurteil des Bundesverfassungsgerichts

Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 aufgrund der mündlichen Verhandlung vom 18. und 19. Oktober 1983 (BvR 209, 269, 362, 420, 440, 484/83) zum Volkszählungsgesetz 1983 (BVerfGE 65, S. 1 f.).

Leitsätze

1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

2. Einschränkungen dieses Rechts auf „informationelle Selbstbestimmung“ sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

3. Bei den verfassungsrechtlichen Anforderungen an derartige Einschränkungen ist zu unterscheiden zwischen personenbezogenen Daten, die in individualisierter, nicht anonymer Form erhoben und verarbeitet werden, und solchen, die für statistische Zwecke sind. Bei den Datenerhebungen für statistische Zwecke kann eine enge und konkrete Zweckbindung der Daten nicht verlangt werden. Der Informationserhebung und -verarbeitung müssen aber innerhalb des Informationssystems zum Ausgleich entsprechende Schranken gegenüberstehen.

4. Das Erhebungsprogramm des Volkszählungsgesetzes 1983 (§ 2 Nr. 1 bis 7, §§ 3 bis 5) führt nicht zu einer mit der Würde des Menschen unvereinbaren Registrierung und Katalogisierung der Persönlichkeit; es entspricht auch den Geboten der Normenklarheit und Verhältnismäßigkeit. Indessen bedarf es zur Sicherung des Rechts auf informationelle Selbstbestimmung ergänzender verfahrensrechtlicher Vorkehrungen für Durchführung und Organisation der Datenerhebung.

5. Die in § 9 Abs. 1 bis 3 des Volkszählungsgesetzes 1983 vorgesehen Übermittlungsregelungen (unter anderem Melderegisterabgleich) verstoßen gegen das allgemeine Persönlichkeitsrecht. Die Weitergabe zu wissenschaftlichen Zwecken (§ 9 Abs. 4 VZG 1983) ist mit dem Grundgesetz vereinbar.

3.1.3 Bundesdatenschutzgesetz

§ 3 Weitere Begriffsbestimmungen

...

(6) 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 bestimmbar natürlichen Person zugeordnet werden können.

(6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(7) Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

...

(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

...

§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
 - b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,
2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und
3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten. Werden personenbezogene Daten beim Betroffenen auf Grund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die

Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

§ 4 a Einwilligung

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(2) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

§ 14 Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

...

9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

§ 28 Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient,

2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder
3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichten dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

...

- (3) Die Übermittlung oder Nutzung für einen anderen Zweck ist auch zulässig:

...

4. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

...

- (5) Der Dritte, dem die Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nicht öffentlichen Stellen nur unter den Voraussetzungen der Absätze 2 und 3 und öffentlichen Stellen nur unter den Voraussetzungen des § 14 Abs. 2 erlaubt. Die übermittelnde Stelle hat ihn darauf hinzuweisen.

- (6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4 a Abs. 3 eingewilligt hat, wenn

...

4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

- (7) Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist ferner zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. Werden zu einem in Satz 1 genannten Zweck Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 3 des Strafgesetzbuches genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Arzt selbst hierzu befugt wäre.

(8) Für einen anderen Zweck dürfen die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) nur unter den Voraussetzungen des Abs. 6 Nr. 1 bis 4 oder des Abs. 7 Satz 1 übermittelt oder genutzt werden. Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.

(9) Organisationen, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, dürfen besondere Arten personenbezogener Daten (§ 3 Abs. 9) erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist. Dies gilt nur für personenbezogene Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4 a Abs. 3 zulässig. Absatz 3 Nr. 2 gilt entsprechend.

§ 30 Geschäftsmäßige Datenerhebung und -speicherung zum Zwecke der Übermittlung in anonymisierter Form

(1) Werden personenbezogene Daten geschäftsmäßig erhoben und gespeichert, um sie in anonymisierter Form zu übermitteln, sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies für die Erfüllung des Zwecks der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.

(2) Die Veränderung personenbezogener Daten ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Veränderung hat, oder
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, soweit nicht das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Veränderung offensichtlich überwiegt.

(3) Die personenbezogenen Daten sind zu löschen, wenn ihre Speicherung unzulässig ist.

(4) § 29 gilt nicht.

(5) § 28 Abs. 6 bis 9 gilt entsprechend.

§ 40 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen

(1) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden.

(2) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbar Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(3) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

1. der Betroffene eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

3.1.4 *Strafgesetzbuch*

§ 202a Ausspähen von Daten

(1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 203 Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,
3. Rechtsanwalt, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,
4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,
- 4a. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,
5. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder
6. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen Verrechnungsstelle

anvertraut worden oder sonst bekannt geworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten,
3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,
4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,
5. öffentlich bestellten Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist oder
6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist

anvertraut worden oder sonst bekannt geworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfasst worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekannt gegeben werden und das Gesetz dies nicht untersagt.

(3) Einem in Absatz 1 Nr. 3 genannten Rechtsanwalt stehen andere Mitglieder einer Rechtsanwaltskammer gleich. Den in Absatz 1 und Satz 1 Genannten stehen ihre berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind. Den in Absatz 1 und den in Satz 1 und 2 Genannten steht nach dem Tod des zur Wahrung des Geheimnisses Verpflichteten ferner gleich, wer das Geheimnis von dem Verstorbenen oder aus dessen Nachlass erlangt hat.

(4) Die Absätze 1 bis 3 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(5) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

§ 204 Verwertung fremder Geheimnisse

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein Betriebs- oder Geschäftsgeheimnis, zu dessen Geheimhaltung er nach § 203 verpflichtet ist, verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 203 Abs. 4 gilt entsprechend.

3.2 Berliner Landesrecht

3.2.1 *Verfassung von Berlin*

Art. 33

Das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, wird gewährleistet. Einschränkungen dieses Rechts bedürfen eines Gesetzes. Sie sind nur im überwiegenden Allgemeininteresse zulässig.

Art. 47

(1) Zur Wahrung des Rechts auf informationelle Selbstbestimmung wählt das Abgeordnetenhaus einen Datenschutzbeauftragten. Er wird vom Präsidenten des Abgeordnetenhauses ernannt und unterliegt dessen Dienstaufsicht.

(2) Das Nähere regelt ein Gesetz.

3.2.2 *Berliner Datenschutzgesetz*

§ 4 Begriffsbestimmungen

(1) Im Sinne dieses Gesetzes sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Entsprechendes gilt für Daten über Verstorbene, es sei denn, dass schutzwürdige Belange des Betroffenen nicht mehr beeinträchtigt werden können.

(3) Im Sinne dieses Gesetzes ist

...

7. Anonymisieren 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,
8. Pseudonymisieren das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

...

§ 5 a Datenverarbeitung

Die Planung, Gestaltung und Auswahl informationstechnischer Produkte und Verfahren haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 6 Zulässigkeit der Datenverarbeitung

- (1) Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn
1. dieses Gesetz oder
 2. eine besondere Rechtsvorschrift sie erlauben oder
 3. der Betroffene eingewilligt hat.

Die Verarbeitung personenbezogener Daten ist nach diesem Gesetz zulässig, wenn wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Satz 1 Nr. 2 gilt nur, wenn die Rechtsvorschrift einen diesem Gesetz vergleichbaren Datenschutz gewährleistet.

- (2) Werden aufgrund einer Rechtsvorschrift des Bundes personenbezogene Daten verarbeitet, ohne dass die Verarbeitung im Einzelnen geregelt ist, finden die §§ 13 bis 15 des Bundesdatenschutzgesetzes Anwendung.

- (3) Wird die Datenverarbeitung auf die Einwilligung des Betroffenen gestützt, so ist dieser in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, aufzuklären. Die Aufklärungspflicht umfasst bei beabsichtigten Übermittlungen auch den Empfänger der Daten sowie den Zweck der Übermittlung. Der Betroffene ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass er die Einwilligung verweigern kann.

- (4) Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, so ist der Betroffene darauf schriftlich besonders hinzuweisen.

- (5) Die Einwilligung des Betroffenen ist nur wirksam, wenn sie auf seiner freien Entscheidung beruht. Sie ist insbesondere unwirksam, wenn sie durch Androhung ungesetzlicher Nachteile oder durch fehlende Aufklärung bewirkt wurde. Soweit besondere Kategorien personenbezogener Daten nach § 6 a Abs. 1 verarbeitet werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

- (6) Die Einwilligung kann auch elektronisch erklärt werden. Es muss dabei sichergestellt werden, dass die Anforderungen zum Nachweis der Authentizität der Einwilligung jenen Anforderungen entsprechen, die für das zu Grunde liegende Verwaltungshandeln verlangt werden.

§ 6 a Verarbeitung besonderer Kategorien personenbezogener Daten

- (1) Personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen oder die die Gesundheit oder das Sexualleben betreffen, dürfen nur verarbeitet werden, wenn angemessene Garantien zum Schutze des Rechtes auf informationelle Selbstbestimmung bestehen und eine besondere Rechtsvorschrift, die den Zweck der Verarbeitung bestimmt, dies erlaubt.

- (2) Die Verarbeitung dieser Daten ist auch zulässig, wenn der Betroffene ausdrücklich eingewilligt hat oder die Verarbeitung zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist und der Betroffene aus rechtlichen oder tatsächlichen Gründen nicht in der Lage ist, seine Einwilligung zu geben.

(3) Die Absätze 1 und 2 finden keine Anwendung, wenn

1. Daten auf der Grundlage von § 2 Abs. 2 oder § 30 dieses Gesetzes verarbeitet werden oder
2. die Datenverarbeitung zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen.

§ 30 Datenverarbeitung für wissenschaftliche Zwecke

(1) Zum Zwecke wissenschaftlicher Forschung dürfen Daten verarbeitende Stellen personenbezogene Daten ohne Einwilligung des Betroffenen nur für bestimmte Forschungsarbeiten übermitteln,

1. soweit dessen schutzwürdige Belange wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden, oder
2. wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann.

Die Übermittlung bedarf der vorherigen Zustimmung der obersten Landesbehörde oder einer von dieser bestimmten Stelle; dies gilt nicht für die öffentlichen Stellen nach § 2 Abs. 3. Die Zustimmung muss den Empfänger, die Art der zu übermittelnden personenbezogenen Daten, den Kreis der Betroffenen und das Forschungsvorhaben bezeichnen und ist dem Berliner Beauftragten für den Datenschutz und Informationsfreiheit mitzuteilen.

(2) Sobald der Forschungszweck dies erlaubt, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern, die Merkmale sind zu löschen, sobald der Forschungszweck erreicht ist.

(3) Eine Verarbeitung der nach Abs. 1 übermittelten Daten zu anderen als Forschungszwecken ist unzulässig. Die nach Abs. 1 Satz 2 übermittelten Daten dürfen nur mit Einwilligung des Betroffenen weiterübermittelt werden.

(4) Soweit die Vorschriften dieses Gesetzes auf den Empfänger keine Anwendung finden, dürfen personenbezogene Daten nur übermittelt werden, wenn sich der Empfänger verpflichtet, die Vorschriften der Abs. 2 und 3 einzuhalten, und sich der Kontrolle des Berliner Beauftragten für Datenschutz und Informationsfreiheit unterwirft.

(5) Die wissenschaftliche Forschung betreibenden öffentlichen Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

- a) der Betroffene eingewilligt hat oder
- b) dieses für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

(6) Unter den Voraussetzungen des Abs. 1 darf die Daten verarbeitende Stelle personenbezogene Daten ohne Einwilligung des Betroffenen selbst zum Zwecke wissenschaftlicher Forschung verarbeiten.

3.3 Hessisches Landesrecht

3.3.1 *Hessisches Datenschutzgesetz*

§ 7 *Zulässigkeit der Datenverarbeitung*

- (1) Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn
 1. eine diesem Gesetz vorgehende Rechtsvorschrift sie vorsieht oder zwingend voraussetzt,
 2. dieses Gesetz sie zulässt oder
 3. der Betroffene ohne jeden Zweifel eingewilligt hat.
- (2) Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Sie muss sich im Falle einer Datenverarbeitung nach Abs. 4 ausdrücklich auch auf die dort genannten Daten beziehen. Wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, ist der Betroffene hierauf schriftlich besonders hinzuweisen. Der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, aufzuklären. Die Aufklärungspflicht umfasst bei beabsichtigten Übermittlungen auch den Empfänger der Daten. Der Betroffene ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass er die Einwilligung verweigern und jederzeit mit Wirkung für die Zukunft widerrufen kann.
- (3) Unzulässig ist eine zu rechtlichen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen führende Entscheidung, wenn sie auf einer Bewertung einzelner Merkmale seiner Person beruht, die ausschließlich durch eine automatisierte Verarbeitung seiner Daten erstellt wurde. Eine Entscheidung nach Satz 1 kann durch Gesetz zugelassen werden, das die Wahrung der berechtigten Interessen des Betroffenen sicherstellt.
- (4) Soweit nicht eine Rechtsvorschrift die Verarbeitung personenbezogener Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben vorsieht oder zwingend voraussetzt, darf eine Verarbeitung nur nach §§ 33 bis 35 und 39 erfolgen. Im Übrigen ist eine Verarbeitung auf Grund dieses Gesetzes nur zulässig, wenn sie ausschließlich im Interesse des Betroffenen liegt und der Hessische Datenschutzbeauftragte vorab gehört worden ist.
- (5) Wenn der Betroffene schriftlich begründet, dass der rechtmäßigen Verarbeitung seiner Daten auf Grund dieses Gesetzes schutzwürdige, sich aus seiner besonderen persönlichen Lage ergebende Gründe entgegenstehen, ist die Verarbeitung nur zulässig, nachdem eine Abwägung im Einzelfall ergeben hat, dass seine Gründe hinter dem öffentlichen Interesse an der Verarbeitung zurückstehen müssen. Dem Betroffenen ist das Ergebnis mit Begründung schriftlich mitzuteilen.
- (6) Wer für den Einsatz oder die wesentliche Änderung eines Verfahrens zur automatisierten Datenverarbeitung zuständig ist, hat vor dem Beginn der Verarbeitung zu untersuchen, ob damit Gefahren für die in § 1 Abs. 1 Nr. 1 geschützten Rechte verbunden sind; dies gilt in besonderem Maße für die in § 7 Abs. 4 genannten Daten. Das Verfahren darf nur eingesetzt werden, wenn sichergestellt ist, dass diese Gefahren nicht bestehen oder durch technische und organisatorische Maßnahmen verhindert werden können. Das Ergebnis der Untersuchung und dessen Begründung sind aufzuzeichnen und dem behördlichen Datenschutzbeauftragten zur Prüfung zuzuleiten.

(7) Die in § 3 Abs. 1 Satz 2 und Abs. 6 genannten Stellen dürfen Daten, die Straftaten betreffen, nur unter behördlicher Aufsicht verarbeiten oder wenn eine Rechtsvorschrift dies vorsieht.

§ 33 Datenverarbeitung für wissenschaftliche Zwecke

(1) Zum Zwecke wissenschaftlicher Forschung dürfen Daten verarbeitende Stellen personenbezogene Daten ohne Einwilligung des Betroffenen im Rahmen bestimmter Forschungsvorhaben verarbeiten, soweit dessen schutzwürdige Belange wegen der Art der Daten, ihrer Offenkundigkeit oder der Art ihrer Verwendung nicht beeinträchtigt werden. Der Einwilligung des Betroffenen bedarf es auch nicht, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen überwiegt und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Im Falle des Satz 2 bedarf die Verarbeitung durch Stellen des Landes der vorherigen Genehmigung der obersten Landesbehörde oder einer von dieser bestimmten Stelle. Die Genehmigung muss den Empfänger, die Art der zu übermittelnden personenbezogenen Daten, den Kreis der Betroffenen und das Forschungsvorhaben bezeichnen und ist dem Hessischen Datenschutzbeauftragten mitzuteilen.

(2) Sobald der Forschungszweck dies erlaubt, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern; die Merkmale sind zu löschen, sobald der Forschungszweck dies zulässt.

(3) Eine Verarbeitung der nach Abs. 1 übermittelten Daten zu anderen als Forschungszwecken ist unzulässig. Die nach Abs. 1 Satz 2 übermittelten Daten dürfen nur mit Einwilligung des Betroffenen weiter übermittelt werden.

(4) Soweit die Vorschriften dieses Gesetzes auf den Empfänger keine Anwendung finden, dürfen personenbezogene Daten nur übermittelt werden, wenn sich der Empfänger verpflichtet, die Vorschriften der Abs. 2 und 3 einzuhalten, und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft.

Anlage 4 – Übersicht über weitere Forschungsregelungen

Der Text der Regelungen ist beim Berliner Datenschutzbeauftragten und beim Hessischen Datenschutzbeauftragten erhältlich oder über Internet direkt abrufbar (verlinkt).

4.1 Bund

4.1.1 Sozialgesetzbuch X

Zweites Kapitel: Schutz der Sozialdaten

Erster Abschnitt: Begriffsbestimmungen

§ 67 Begriffsbestimmungen

§ 67b Zulässigkeit der Datenverarbeitung und -nutzung

§ 67c Datenspeicherung, -veränderung und -nutzung

§ 67d Übermittlungsgrundsätze

§ 75 Übermittlung von Sozialdaten für die Forschung und Planung

§ 76 Einschränkung der Übermittlungsbefugnis bei besonders schutzwürdigen Sozialdaten

§ 77 Einschränkung der Übermittlungsbefugnis ins Ausland sowie an über- und zwischenstaatliche Stellen

§ 78 Zweckbindung und Geheimhaltungspflicht des Empfängers

§ 100a Übermittlung für die Forschung zur Bekämpfung von Berufskrankheiten

4.1.2 Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz – BStatG)

§ 16 Geheimhaltung

§ 22 Strafvorschrift

§ 23 Bußgeldvorschrift

4.1.3 Gesetz über die Sicherung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz – BArchG)

4.1.4 Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz – BZRG)

§ 42 Auskunft in besonderen Fällen

4.1.5 Strafprozessordnung (StPO)

- § 476 Wissenschaftliche Forschung
- § 477 Auskünfte
- § 487 Übermittlung
- § 489 Berichtigung, Löschung, Sperrung

4.1.6 Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz – StUG)

- § 1 Zweck und Anwendungsbereich des Gesetzes
- § 4 Zulässigkeit der Verwendung der Unterlagen des Staatssicherheitsdienstes durch öffentliche und nicht-öffentliche Stellen
- § 32 Verwendung von Unterlagen für die Aufarbeitung der Tätigkeit des Staatssicherheitsdienstes
- § 33 Verfahren
- § 42 Kosten

4.1.7 Umweltinformationsgesetz (UIG)

- § 8 Ausschluss und Beschränkungen des Anspruchs zum Schutz privater Belange

4.1.8 Straßenverkehrsgesetz

- § 2c Registrierung der Fahrerlaubnis während der Probezeit, Datenschutz
- § 2d Übermittlung der Registrierdaten für wissenschaftliche, statistische und gesetzgeberische Zwecke
- § 38 Übermittlung von Fahrzeugdaten und Halterdaten für wissenschaftliche, statistische, planerische und gesetzgeberische Zwecke

4.1.9 Gesetz über die Statistik der Straßenverkehrsunfälle (Straßenverkehrsunfallstatistikgesetz – StVUnfStatG)

- § 5

4.1.10 Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften

- § 150b Auskunft für die wissenschaftliche Forschung

4.1.11 Strafvollzugsgesetz (StVollzG)

- § 186 Auskunft und Akteneinsicht für wissenschaftliche Zwecke

4.2 Berlin

4.2.1 Berliner Informationsfreiheitsgesetz

4.2.2 Meldegesetz Berlin

- § 25 Datenübermittlungen an andere Behörden oder sonstige öffentliche Stellen
- § 28 Melderegisterrückkunft
- § 29 Melderegisterrückkünfte in besonderen Fällen

4.2.3 Landesstatistikgesetz

- § 16 Geheimhaltung
- § 24 Geheimhaltung, Übermittlung von Ergebnissen
- § 25 Voraussetzungen und Empfänger

4.2.4 Gesetz über die Sicherung und Nutzung von Archivgut des Landes Berlin (Archivgesetz des Landes Berlin – ArchGB)

- § 1 Organisation und Zuständigkeit im Archivwesen im Land Berlin
- § 2 Aufgaben des Landesarchivs Berlin
- § 3 Archivgut
- § 4 Aussonderung und Anbietetung von Archivgut
- § 5 Daten von ehemaligen Einrichtungen der DDR
- § 6 Übernahme des Archivgutes
- § 7 Sicherung des Archivgutes
- § 8 Nutzung des Archivgutes
- § 9 Recht auf Auskunft und Gegendarstellung
- § 10 Landesbildstelle
- § 11 Sonstige öffentliche Archive
- § 12 Änderung des Zweiten Gesetzes zum Abschluss der Entnazifizierung
- § 13 Inkrafttreten

4.2.5 Landeskrankenhausgesetz (LKG)

- § 26 Krankengeschichten, Datenschutz

4.2.6 Berufsordnung der Ärztekammer Berlin

- § 3 Schweigepflicht

4.2.7 Bereichsspezifische Regelungen für die Verarbeitung personenbezogener Daten (Artikelgesetz)

Artikel XIII Änderung des Schulgesetzes für Berlin

§ 5a Datenschutz

4.3 Hessen

4.3.1 Hessisches Meldegesetz

§ 31 Datenübermittlungen an andere Behörden oder sonstige öffentliche Stellen

§ 34 Allgemeine Melderegisterauskunft

§ 35 Melderegisterauskünfte in besonderen Fällen

4.3.2 Landesstatistikgesetz

§ 16 Geheimhaltung

4.3.3 Landesarchivgesetz

§ 2 Archivgut des Landes

§ 3 Archivgut des Bundes

§ 4 Kommunales Archivgut

§ 5 Sonstiges öffentliches Archivgut

§ 6 Begriffsbestimmungen

§ 7 Aufgaben der öffentlichen Archive

§ 14 Allgemeines

§ 15 Schutzfristen

§ 16 Einschränkung der Nutzung von Archivgut in besonderen Fällen

4.3.4 Landeskrankenhausgesetz

§ 12 Datenschutz im Krankenhaus

4.3.5 Hessisches Schulgesetz

§ 84 Wissenschaftliche Forschung

4.3.6 Hessisches Krebsregistergesetz

- § 1 Zweck und Regelungsbereich
- § 2 Meldungen
- § 3 Meldungsinhalte
- § 4 Vertrauensstelle
- § 5 Registerstelle
- § 7 Übermittlung von Forschungszwecke

4.3.7 Berufsordnung für die Ärztinnen und Ärzte in Hessen

- § 9 Schweigepflicht

Anlage 5 – Internationale Vereinbarungen/Rechtsvorschriften/ Erklärungen

5.1 EG-Datenschutzrichtlinie

5.2 Erklärung der European Science Foundation zu der Verwendung personenbezogener Daten zu Forschungszwecken

5.3 Europarat-Empfehlung zum Schutz personenbezogener Daten für Zwecke der wissenschaftlichen Forschung und Statistik (Nr. R [83] 10)

Anlage 6 – Deutsche Arbeitsgemeinschaft für Epidemiologie (DAE)

Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Epidemiologie und Datenschutz

(Umlaufbeschluss der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Mai 1998)

Inhaltsübersicht:

Einleitung

1. Rechtliche Rahmenbedingungen für die Forschung mit personenbezogenen Daten

- 1.1 Forschung mit anonymisierten Daten
- 1.2 Forschung mit Einwilligung der Betroffenen
- 1.3 Forschung mit personenbezogenen Daten ohne Einwilligung der Betroffenen

2. Forschungsansätze in der Epidemiologie, Datenbedarf und Rechtsgrundlagen der Datenverarbeitung

3. Typische Problemfelder

- 3.1 Zweckbindung von personenbezogenen Daten
- 3.2 Löschung der Daten nach Beendigung des Forschungsvorhabens
- 3.3 Weitergabe anonymisierter Daten
- 3.4 Optimale Gestaltung der Einverständniserklärung bzw. des Antrags auf Übermittlung der Daten
- 3.5 Verknüpfung personenbezogener Datensätze (record linkage) z. B. bei Kohortenstudien
- 3.6 Nutzung der amtlichen Statistik
- 3.7 Aufbewahrung von Daten der amtlichen Statistik
- 3.8 Nutzung von Krebsregistern für Fall-Kontroll-Studien
- 3.9 Datenschutzfragen bei bundesweiten Studien