5 | Output
5. Berufungsperiode

RatSWD.
Rat für Sozial- und
WirtschaftsDaten

Handreichung Datenschutz

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Inhaltsverzeichnis

1 Einleitung 5

2 Datenschutzrechtliche Grundsätze in Deutschland 6
2.1 Forschungsfreiheit und informationelle Selbstbestimmung 6
2.2 Verbot mit Erlaubnisvorbehalt 6
2.3 Grundsätze bei wissenschaftlich bedingten Eingriffen in das informationelle Selbstbestimmungsrecht 6
2.4 Einwilligungsprinzip 7
2.5 Zweckbindungsprinzip 8

3 Rechtlicher Rahmen des Datenschutzes 9
3.1 Verfassungsrechtlicher Rahmen 9
3.2 Bundesdatenschutzgesetz (BDSG) und Landesdatenschutzgesetze (LDSG) 9
3.3 Sozialgesetzbuch (SGB) 10
3.4 Bundesstatistikgesetz (BStatG) 11
3.5 Weitere spezialgesetzliche Vorschriften 11
3.6 Europäischer Rechtsrahmen: Ausblick 12

4 Grundbegriffe des Datenschutzes für die Forschung 13
4.1 Personenbezogene Daten 13
4.2 Sensible personenbezogene Daten 13
4.3 Anonymisieren 14
4.4 Pseudonymisieren 15
4.5 Datenerhebung, -verarbeitung und -nutzung 16
4.6 Verantwortliche Stelle 16
4.7 Datentreuhänder 16
4.8 Technische und organisatorische Maßnahmen 17
4.9 Verfahrensverzeichnis 17

5 Datenschutzrechtliche Aspekte bei der Feldarbeit 18
5.1 Erhebung und Verarbeitung personenbezogener Daten auf der Grundlage einer Einwilligung der Betroffenen 18
5.2 Datenschutzrechtliche Anforderungen bei der Befragung spezieller Personengruppen 20
5.3 Besonderheiten der Einwilligung bei unterschiedlichen Erhebungsarten 20
5.4 Datenverarbeitung und -speicherung während der Feldarbeit 21
5.5 Umgang mit Verweigerungen, Widerruf von Einwilligungen, Sperrung und Löschung von Daten 22

6 Datenschutzrechtliche Aspekte nach der Feldarbeit 23
6.1 Datenaufbereitung, Datenanalyse: Verarbeitung der Daten nach der Feldphase 23
6.2 Datenpublikation: Verwendung von Daten in Publikationen 23
6.3 Datenaufbewahrung und -archivierung 24
6.4 Sekundärdatennutzung 25

Literaturverzeichnis 27

Anhang 29

Abkürzungsverzeichnis

AGR	Anschriften- und Gebäuderegister
ADM	Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V.
BA	Bundesagentur für Arbeit
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte/r für den Datenschutz und die Informationsfreiheit
BMAS	Bundesministerium für Arbeit und Soziales
BMBF	Bundesministerium für Bildung und Forschung
BMG	Bundesministerium für Gesundheit
BStatG	Bundesstatistikgesetz
BVerfG	Bundesverfassungsgericht
CAPI	Computer-Assisted Personal Interview
CATI	Computer-Assisted Telephone Interview
CAWI	Computer-Assisted Web Interview
DFG	Deutsche Forschungsgemeinschaft
EU-DSGVO	EU-Datenschutz-Grundverordnung
FDZ	Forschungsdatenzentrum
GG	Grundgesetz
GWP	Gute Wissenschaftliche Praxis
IAB	Institut für Arbeitsmarkt- und Berufsforschung
IP	Internet Protocol
IT	Informationstechnik
i.V.m.	in Verbindung mit
KDFV	Kontrollierte Datenfernverarbeitung
KVI	Kommission zur Verbesserung der informationellen Infrastruktur zwischen Wissenschaft und Statistik
LDSG	Landesdatenschutzgesetz
PUF	Public Use File
RatSWD	Rat für Sozial- und Wirtschaftsdaten
SGB	Sozialgesetzbuch
SUF	Scientific Use File

1 Einleitung

Der Rat für Sozial- und Wirtschaftsdaten (RatSWD) ist ein unabhängiges Gremium bestehend aus empirisch arbeitenden Wissenschaftlerinnen und Wissenschaftlern sowie Vertreterinnen und Vertretern von Datenproduzenten. Er wurde 2004 vom Bundesministerium für Bildung und Forschung eingerichtet, um die Forschungsdateninfrastruktur für die empirische Forschung nachhaltig zu verbessern und somit zu ihrer internationalen Wettbewerbsfähigkeit beizutragen. Der RatSWD arbeitet an der Schnittstelle von Wissenschaft, Datenproduktion und Datenschutz. Zu seinen Aufgaben gehört es, Wissenschaft und Politik zu beraten. Er bündelt die Kompetenz von 30 Forschungsdatenzentren. Im Rahmen dieses Mandates hat der RatSWD während seiner fünften Berufungsperiode (2014 – 2017) die vorliegende Handreichung zum Thema Datenschutz erstellt. Hierbei steht der Umgang mit personenbezogenen Daten im Rahmen sozial-, verhaltens- und wirtschaftswissenschaftlicher Forschung im Zentrum des Interesses.

Ziel dieser Handreichung ist es, allen Interessierten und insbesondere den Forschenden aus den Sozial-, Verhaltens- und Wirtschaftswissenschaften die für die empirische Forschung relevanten Regelungen des Datenschutzes in Deutschland näher zu bringen. Im ersten Teil der Handreichung werden datenschutzrechtliche Grundsätze erläutert, der gesetzliche Rahmen des Datenschutzes in Deutschland dargestellt und Grundbegriffe erklärt. Im zweiten Teil bespricht diese Handreichung solche Aspekte des Datenschutzes, die bei der Vorbereitung, Durchführung und nach dem Abschluss von empirischen Forschungsprojekten relevant sind.

Insgesamt soll die Handreichung kein umfassendes Kompendium, sondern eine knappe Hinführung bieten. Weiterführende Literaturhinweise finden sich im Text. Der Text stellt den Rechtsstand zum 30. Juni 2016 dar, d. h. vor Wirksamwerden der Europäischen Datenschutzgrundverordnung am 25. Mai 2018 sowie ihrer nationalen Umsetzung.

2 Datenschutzrechtliche Grundsätze in Deutschland

In diesem einleitendem Abschnitt werden die für den Datenschutz und die Forschung in Deutschland relevanten Grundsätze erläutert.

2.1 Forschungsfreiheit und informationelle Selbstbestimmung

In Deutschland ist die Forschungsfreiheit ein Recht mit Verfassungsrang. Artikel 5 Abs. 3 Satz 1 des Grundgesetzes zufolge gilt: „Kunst und Wissenschaft, Forschung und Lehre sind frei." Sie dürfen somit keiner willkürlichen Einschränkung unterworfen werden. Grundrechtsträger sind also auch Beschäftigte an wissenschaftlichen Hochschulen und außeruniversitären Forschungseinrichtungen, die sozial-, verhaltens- und wirtschaftswissenschaftliche Forschungsprojekte durchführen.

Sofern diese Forschung eine Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten umfasst, müssen auch die Rechte der Betroffenen (Daten-Subjekte) und insbesondere deren Recht auf informationelle Selbstbestimmung in einer angemessenen Weise berücksichtigt werden. Bei diesem Recht handelt es sich um ein aus dem allgemeinen Persönlichkeitsrecht abgeleitetes Grundrecht, demzufolge Einzelne grundsätzlich befugt sind, selbst über die Preisgabe und Verwendung ihrer persönlichen Daten zu bestimmen (Metschke und Wellbrock 2002, S. 9). Kollidiert die Forschungsfreiheit, wie in diesem Fall, mit einem anderen Grundrecht, so muss ein Ausgleich gefunden werden, der beiden Grundrechten möglichst weitreichende Geltung verschafft (praktische Konkordanz).

2.2 Verbot mit Erlaubnisvorbehalt

Grundsätzlich ist in Deutschland die Erhebung, Verarbeitung und Nutzung personenbezogener Daten untersagt und nur unter bestimmten Voraussetzungen zulässig. Der Gesetzgeber hat diesbezüglich Regelungen getroffen und an verschiedenen Stellen Erlaubnistatbestände bzw. Rechtsgrundlagen für die Arbeit mit personenbezogenen Daten definiert (vgl. Kapitel 3).

2.3 Grundsätze bei wissenschaftlich bedingten Eingriffen in das informationelle Selbstbestimmungsrecht

Sofern bei Forschungsprojekten personenbezogene Daten erhoben, verarbeitet oder genutzt werden, sind die Interessen der Betroffenen gegenüber denen der Wissenschaft abzuwägen. Folgende Aspekte sind dabei relevant:[1]

a) Gemeinschaftsinteresse: Forschende sind angehalten zu prüfen, ob das Forschungsvorhaben einem legitimen Gemeinschaftsinteresse dient. Zum Beispiel liegt ein Forschungsvorhaben, das bereits inhaltlich gegen andere Gesetze verstößt, nicht im Gemeinschaftsinteresse und muss daher nicht erst am Recht auf informationelle Selbstbestimmung scheitern (Metschke und Wellbrock 2002, S. 11).

b) Geeignetheitsgrundsatz: Es muss unstrittig sein, dass ein Eingriff in Persönlichkeitsrechte, der durch Erhebung, Verarbeitung und Nutzung personenbezogener Daten entsteht, auch dazu geeignet ist, zur Klärung der Forschungsfrage beizutragen. Insofern Daten beispielsweise lediglich auf Vorrat hinterlegt werden, ist dies in Frage gestellt.

1 Weitere detaillierte Informationen finden sich bei BfDI (2016a).

c) Erforderlichkeitsgrundsatz: Personenbezogene Daten sollten nur dann erhoben, verarbeitet oder genutzt werden, wenn der Forschungszweck nicht auf andere Art und Weise erreicht werden kann. Könnten Forschungsdaten über ein Forschungsdatenzentrum (FDZ) sekundär genutzt werden, wäre eine Primärerhebung beispielsweise nicht erforderlich (vgl. Häder 2009, S. 9).

d) Übermaßverbot/Verhältnismäßigkeit: Das Übermaßverbot verlangt ein angemessenes Verhältnis zwischen der erforderlichen Beeinträchtigung der Betroffenen und dem angestrebten Untersuchungszweck (Häder 2009, Metschke und Wellbrock 2002). Demnach muss ein Eingriff in die Privatsphäre des Datengebers so weit wie möglich minimiert werden und es sollten beispielsweise nicht mehr geeignete Daten erhoben werden, als erforderlich.

e) Wahl des mildesten Mittels: Unter allen möglichen geeigneten Mitteln der Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist dasjenige zu wählen, welches die schwächste Form des Grundrechtseingriffs darstellt. Dies bezieht sich sowohl auf die Art und die Menge der zu verarbeitenden Daten als auch auf den Kreis der Personen, die Kenntnis der personenbezogenen Daten erhalten (vgl. Metschke und Wellbrock 2002, S. 11 f.).

f) Datenvermeidung und Datensparsamkeit: Ein erweitertes Verständnis von Datenschutz findet darin Ausdruck, dass bereits vor der Ausgestaltung von Datenerhebungen und -verarbeitungen darauf hingewirkt wird, keine oder möglichst wenig personenbezogene Daten zu verwenden. Dies ist beispielsweise in § 3a Bundesdatenschutzgesetz (BDSG) konkretisiert: „Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen."

2.4 Einwilligungsprinzip

„Das Einwilligungsprinzip bestimmt, dass personenbezogene Daten nicht ohne Einwilligung der Betroffenen be- oder verarbeitet werden dürfen, es sei denn, die Verarbeitung erfolgt aufgrund und im Rahmen einer Rechtsnorm." (KVI 2001, S. 19). Fehlt also eine solche Rechtsvorschrift, darf die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nur mit der vorherigen Zustimmung des bzw. der Betroffenen erfolgen. Liegt eine solche Einwilligung in gültiger Form vor, so ist das Arbeiten mit personenbezogenen Daten unter der Maßgabe der in Abschnitt 2.3 aufgeführten Grundsätze datenschutzrechtlich grundsätzlich unproblematisch.

Die Voraussetzungen für die Gültigkeit einer Einwilligung werden vom Gesetzgeber definiert (z. B. § 4a BDSG, vgl. auch Kapitel 5.1.1). Eine gültige Einwilligungserklärung muss insbesondere auf der freien Willensentscheidung der Betroffenen beruhen. Hierfür müssen diese über Grund und Durchführung der Datenerhebung, -verarbeitung und -nutzung in einer für die Betroffenen verständlichen Art und Weise informiert werden. Der Einwilligungstext muss hierzu ggf. hinsichtlich unterschiedlicher Betroffenengruppen (beispielsweise in Hinblick auf Altersgruppen oder Kompetenzen) angepasst werden, wobei die Einsichtsfähigkeit der Betroffenen ausschlaggebend ist (vgl. Metschke und Wellbrock 2002, Gerling 2008). Darüber hinaus müssen Betroffene über die Bedeutung ihrer Einwilligung aufgeklärt werden. Hierzu gehören auch Informationen darüber, dass die Einwilligung verweigert oder mit Wirkung für die Zukunft widerrufen werden kann (vgl. zum Umgang mit Widerrufen Kapitel 5.5 und BfDI 2005, S.13 f.).

Für bestimmte Fälle, in denen Daten auch ohne Einwilligung der Betroffenen erhoben, verarbeitet oder genutzt werden können, hat der Gesetzgeber Erlaubnistatbestände definiert. Relevant für die Forschung sind hier u. a. solche Regelungen, die die Ziehung von Einwohnermeldeamtsstichproben ohne Einwilligung betreffen.[2]

2 Beispielsweise beziehen sich Institute der Markt- und Meinungsforschung insbesondere bei der Anforderung von Anschriften aus den Einwohnermelderegistern zur Durchführung repräsentativer Umfragen auf § 30a BDSG. Hier sowie bei Gruppenauskünften aus Melderegistern im Allgemeinen wird (teilweise) eine Unbedenklichkeitsbescheinigung der zuständigen Datenschutzaufsichtsbehörde benötigt bzw. angefordert.

Erfolgt keine Einwilligung oder sind die Betroffenen gesetzlich verpflichtet ihre Angaben preiszugeben (z. B. im Rahmen amtlicher Erhebungen), so sind die Betroffenen in ihren Persönlichkeitsrechten besonders zu schützen. Dies erfolgt im Rahmen der amtlichen Statistik beispielsweise durch die Vorgaben des Statistikgeheimnisses und die Übermittlung von faktisch anonymisierten Daten zu wissenschaftlichen Zwecken (bei zweckgebundener, vertraglich vereinbarter, zeitlich befristeter Nutzung).

In Hinblick auf Sozialdaten ist eine Übermittlung nach § 75 SGB X für bestimmte wissenschaftliche Vorhaben (d. h. zweckgebunden) möglich, wenn das schutzwürdige Interesse der Betroffenen nicht beeinträchtigt wird oder das öffentliche Interesse an der Forschung das Geheimhaltungsinteresse der Betroffenen erheblich überwiegt. Eine solche Übermittlung ist – sofern eine nachträgliche Einwilligung durch die Betroffenen nicht zumutbar ist – durch die oberste Bundes- und Landesbehörde zu genehmigen.

Für die öffentlichen Stellen des Bundes finden sich vergleichbare Regelungen für die Datenverarbeitung und -nutzung ohne Einwilligung im Bundesdatenschutzgesetz (§ 14 BDSG).[3] Diese fordern Erforderlichkeit der Daten, ein wissenschaftliches Interesse an der Durchführung des Forschungsvorhabens, das die Interessen der Betroffenen erheblich überwiegt, sowie dass der Forschungszweck anders nicht oder nur mit unverhältnismäßig hohem Aufwand erreicht werden kann (Forschungsprivileg).

2.5 Zweckbindungsprinzip

Personenbezogene Daten dürfen nur für den Zweck, für den sie erhoben wurden, verarbeitet und genutzt werden (Zweckidentität). Ausgeschlossen ist somit eine Datenerhebung und -speicherung auf Vorrat. „Eine Datenverarbeitung zu einem anderen als dem ursprünglich festgelegten Zweck ist als Zweckänderung oder Zweckdurchbrechung nur auf gesetzlicher Grundlage oder mit Einwilligung der Betroffenen zulässig." (BfDI 2005).

Die Zweckbindung ist das entscheidende Sicherungsinstrument für Betroffene. Der beispielsweise mit einer Einwilligung legitimierte Zweck begrenzt die Möglichkeit der datenverarbeitenden Stelle, über die Daten der Betroffenen verfügen zu können. Die Benennung klar erkennbarer Zwecke ist dabei Voraussetzung für wirksame Einwilligungserklärungen. Eine Einwilligung, bei der Betroffene nicht erkennen können, zu welchem Zweck ihre Daten verwendet werden, ist unwirksam.

Für die wissenschaftliche Forschung ist jedoch eine genaue und detaillierte Angabe der Zwecke nicht immer möglich (vgl. hierzu auch Kapitel 5.1.2). Nach Metschke und Wellbrock ist insofern „bei der Verarbeitung personenbezogener Daten im Wissenschaftsbereich […] eine weitere Formulierung des Zwecks als in anderen Lebensbereichen vertretbar und nicht unangemessen." (2002, S. 27), da diese der wissenschaftlichen Arbeitsweise entspricht. Im internationalen Sprachgebrauch wird in diesem Zusammenhang der Begriff des *broad consent* diskutiert. Diese weite Zweckbindung schließt auch Datennutzungen ein, die zum Zeitpunkt der Einwilligung noch nicht präzise und im Detail definiert werden können (vgl. Sheehan 2011).[4]

Soweit der Zweck jedoch nachträglich geändert werden soll, muss eine Einwilligung des bzw. der Betroffenen eingeholt werden (vgl. Metschke und Wellbrock 2002, S. 27 ff.). Insbesondere ist dabei zu beachten, dass gemäß § 40 BDSG und entsprechenden Normen der einzelnen Landesdatenschutzgesetze (eine Auflistung findet sich bei Gola et al. 2015) für Forschungszwecke erhobene und übermittelte Daten nur für diese Zwecke verarbeitet oder genutzt werden dürfen.

In Hinblick auf die wissenschaftliche Sekundärnutzung von Daten hat der Gesetzgeber an verschiedenen Stellen die rechtlichen Voraussetzungen für Ausnahmen vom Zweckbindungsprinzip geschaffen (vgl. Kapitel 3).

3 Die Regelungen für privatrechtlich Organisierte finden sich in § 28 Abs. 6 bzw. Abs. 9 BDSG.

4 In der EU-Datenschutzgrundverordnung wird die Einwilligung in Artikel 7 geregelt und in den Erwägungsgründen 32 und 33 erläutert.

3 Rechtlicher Rahmen des Datenschutzes

In Deutschland finden sich datenschutzrechtliche Vorgaben in unterschiedlichen Gesetzen (Bundes- und Landesgesetze sowie bereichsspezifische Spezialgesetze), was die Situation für Forschende unübersichtlich macht. Vor der Durchführung der eigenen Forschung, die eine Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten beinhaltet, sollten sich Forschende informieren, welche Rechtsgrundlage für sie gültig ist. Hierfür ist in der Regel der Sitz der Stelle, bei dem das Projekt durchgeführt wird, entscheidend.

Der Anhang zeigt beispielhaft, auf welcher rechtlichen Basis die Daten der vom RatSWD akkreditierten Forschungsdatenzentren bereitgestellt werden.

3.1 Verfassungsrechtlicher Rahmen

Ein Recht auf Datenschutz ist im deutschen Grundgesetz nicht explizit verankert, leitet sich jedoch aus Artikel 2 Abs. 1 GG (Recht auf freie Entfaltung der Persönlichkeit) in Verbindung mit Artikel 1 GG (Schutz der Menschenwürde) des Grundgesetzes ab.[5]

Im europäischen Recht werden Artikel 8 (Recht auf Achtung des Privat- und Familienlebens) der Europäischen Menschenrechtskonvention von 1950 und Artikel 8 der Europäischen Grundrechtecharta von 2000 als einschlägig angesehen.

3.2 Bundesdatenschutzgesetz (BDSG) und Landesdatenschutzgesetze (LDSG)

Der Zweck der Datenschutzgesetze ist es, Einzelne davor zu schützen, dass sie durch den Umgang Dritter mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt werden (z. B. § 1 BDSG). Diese Gesetze kommen erst zur Anwendung, wenn und sofern speziellere Normen (z. B. Bundesstatistikgesetz, Sozialgesetzbuch) Regelungslücken aufweisen (Subsidiaritätsprinzip). Inhaltlich regeln das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze die Erhebung, Verarbeitung und Nutzung personenbezogener Daten (z. B. § 3 BDSG) sowie die Rechte und Pflichten von Datenschutzbeauftragten (z. B. § 4 f. BDSG).

Ein zentraler Regelungsgrundsatz der Gesetze in Hinblick auf die Forschung ist das sogenannte Forschungsprivileg (z. B. § 14 Abs. 2 Nr. 9 BDSG und für privatrechtlich Organisierte § 28 Abs. 2, 6 und 9 BDSG). Demnach ist die Verwendung personenbezogener Daten zur Durchführung wissenschaftlicher Forschung zulässig, wenn dies erforderlich ist, das wissenschaftliche Interesse das Interesse der Betroffenen erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

5 Das Recht auf Datenschutz bekam 1983 mit dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfG) Verfassungsrang. Das BVerfG etablierte damit das sogenannte Recht auf informationelle Selbstbestimmung, welches gewährleistet, dass einzelne Bürgerinnen und Bürger grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten bestimmen dürfen. Das BVerfG sieht die freiheitlich demokratische Gesellschaftsordnung als gefährdet an, wenn Einzelne nicht gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe ihrer persönlichen Daten geschützt sind.

Das Bundesdatenschutzgesetz gilt für öffentliche Stellen und Forschungseinrichtungen des Bundes sowie für privatrechtliche Forschungseinrichtungen. Für öffentliche Stellen und Forschungseinrichtungen des Bundes übt der/die Bundesbeauftragte für den Datenschutz und die Informationssicherheit (BfDI) die Aufsicht aus, für öffentliche Stellen des Landes, für überwiegend öffentlich getragene und für die privaten Forschungseinrichtungen die jeweils zuständige Aufsichtsbehörde des Landes (in der Regel die jeweiligen Landesdatenschutzbeauftragten). Die Landesdatenschutzgesetze gelten für öffentliche Stellen der Länder und Kommunalverwaltungen, dazu gehören Forschungseinrichtungen der jeweiligen Länder, d. h. Hochschulen und Fachhochschulen. Landesdatenschutzgesetze regeln u. a. auch die Rolle der Landesdatenschutzbeauftragten.

3.3 Sozialgesetzbuch (SGB)

Die datenschutzbezogenen Normen des Sozialgesetzbuches haben aufgrund der Subsidiarität des BDSG Vorrang vor den allgemeinen Datenschutznormen von Bund und Ländern. Das zehnte Buch des Sozialgesetzbuchs (SGB X) regelt Verwaltungsverfahren und widmet sich dabei auch dem Schutz von personenbezogenen Daten (Details bei BMAS 2015, Kapitel 10).

Das SGB X bezieht sich auf sogenannte Sozialdaten, d. h. Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, die von einer in § 35 SGB I genannten Stelle erhoben, verarbeitet oder genutzt werden (§ 67 SGB X). Für Sozialdaten (beispielsweise der Renten- und Arbeitslosenversicherung), die als besonders schutzwürdige personenbezogene Daten gelten, ist ein Sozialgeheimnis (§ 35 SGB I) definiert.

Eine Übermittlung solcher Sozialdaten ist nur zulässig, wenn der oder die Betroffene eingewilligt hat oder wenn eine gesetzliche Übermittlungsbefugnis vorliegt; ein zulässiger Zweck ist beispielhaft die Erstellung von statistischen Datengrundlagen gemäß § 79 SGB IV. Als spezialgesetzliche Norm erlaubt § 282 Abs. 7 SGB III dem Institut für Arbeitsmarkt- und Berufsforschung (IAB), faktisch anonymisierte Daten (Scientific Use Files) für Zwecke der Arbeitsmarkt- und Berufsforschung an Forschungseinrichtungen zu übermitteln. Dabei müssen die Forschungseinrichtungen die Datensicherheit nachweisen und die Daten nach Beendigung des Forschungsprojektes löschen. Die generelle Norm zur Übermittlung von Daten an die Forschung ist § 75 SGB X, der gestattet Sozialdaten zu übermitteln, wenn sie für ein bestimmtes Forschungsvorhaben im Sozialleistungsbereich oder in der wissenschaftlichen Arbeitsmarkt- und Berufsforschung erforderlich sind. Die Genehmigung erfolgt durch die oberste Bundes- oder Landesbehörde (Hochfellner et al. 2012b).[6] Bei jeder Übermittlung wird vom Datenschutz geprüft, ob und in welchem Umfang die Übermittlung personenbezogener Daten notwendig ist. In der Regel werden unmittelbar personenbeziehbare Daten wie Namen, Adressen und Geburtsdaten nicht übermittelt, da sie für das Forschungsvorhaben nicht erforderlich sind. Auch Daten, bei denen diese potentiellen Identifikatoren entfernt wurden, sind in ihrer Abstufung noch nicht faktisch anonymisiert (vgl. Kapitel 4.3). Am Forschungsdatenzentrum (FDZ) der Bundesagentur für Arbeit (BA) im IAB werden diese Daten als schwach anonymisiert bezeichnet. Der Datenschutz wird bei der Übermittlung durch das restriktive Arbeiten an Gastwissenschaftlerarbeitsplätzen sichergestellt, wenn es sich um Daten handelt, die über das FDZ der BA im IAB angeboten werden (als Beispiel vgl. Hochfellner et al. 2012a). Auch Daten, die nicht über das FDZ der BA im IAB angeboten werden, können über § 75 SGB X über das IAB beantragt werden.

Daten, die dem SGB unterliegen, werden beim FDZ der BA im IAB und im FDZ der Rentenversicherung angeboten.

6 Zu den prohibitiven Wirkungen der Regelung des § 75 SGB X für die Gesundheitsforschung und den Aufbau von Gesundheitsdatenbanken in Deutschland vgl. BIPS (2016) sowie BfDI (2015).

3.4 Bundesstatistikgesetz (BStatG)

Daten der Statistischen Ämter des Bundes und der Länder unterliegen dem Statistikgeheimnis (§ 16 BStatG). Grundsätzlich sind Einzelangaben über persönliche und sachliche Verhältnisse, die im Rahmen der amtlichen Statistik erhoben werden, geheim zu halten, sofern es keine Ausnahmeregelung dafür gibt.

Einzeldaten der Statistischen Ämter dürfen unter bestimmten Voraussetzungen an ausgewählte externe Stellen übermittelt werden. Hierbei gelten klare Zweckbestimmungen zur Verwendung der Daten und besondere Regelungen zur Sicherstellung der Geheimhaltung. Im Folgenden wird nur auf die Übermittlung für wissenschaftliche Zwecke nach § 16 Abs. 6 BStatG eingegangen.

Erlaubt sind demzufolge u. a. die Übermittlung von faktisch anonymisierten Daten sowie der Zugang zu formal anonymisierten Einzelangaben innerhalb der Statistischen Ämter des Bundes und der Länder an die Wissenschaft. Zur Wissenschaft gehören Universitäten und Hochschulen sowie Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung. Übermittelt werden dürfen Daten zweckgebunden für die Durchführung wissenschaftlicher Projekte. Nach Beendigung des Vorhabens sind die Daten zu löschen (§ 16 Abs. 8 BStatG). Die mit den Daten arbeitenden Forschenden müssen nach § 16 Abs. 7 BStatG auf die statistische Geheimhaltung verpflichtet werden. Für sie gilt ebenfalls die verlängerte Geheimhaltungspflicht nach § 16 Abs. 10 BStatG, d. h. die Geheimhaltungspflicht geht über das Ende ihrer Tätigkeit hinaus. In einzelvertraglichen Regelungen zwischen der Einrichtung und den statistischen Ämtern wird u. a. die Pflicht der Forschenden zur Geheimhaltung geregelt; bei Vertragsverletzungen kommt eine Vertragsstrafe zum Tragen.[7]

3.5 Weitere spezialgesetzliche Vorschriften

Ebenso wie das Bundesstatistikgesetz oder das Sozialgesetzbuch haben bereichsspezifische Gesetze/spezialgesetzliche Vorschriften Vorrang vor den Bundes- und Landesdatenschutzgesetzen. So sind beispielsweise für Erhebungen an Schulen Schulgesetze (amtliche Verwaltungsvorschriften, Schulordnungen einzelner Schularten) zu beachten. Weitere bereichsspezifische Gesetze mit Vorschriften zum Datenschutz in der Forschung sind u. a. das Bundeskrebsregistergesetz, die Landeskrankenhausgesetze oder die Landesarchivgesetze. [8]

7 Die Zusammenführung von Personen- oder Haushaltsdaten wird implizit durch den § 21 BStatG (Verbot der Reidentifizierung) verboten, es sei denn, ein einzelstatistisches Gesetz erlaubt es explizit. Im Bereich der Unternehmensdaten ist seit 2005 ein Zusammenführen von unterschiedlichen Wirtschafts- und Umweltdaten auf der rechtlichen Grundlage des § 13a BStatG möglich. Seit Juli 2016 ist es auf gleicher gesetzlicher Grundlage zudem möglich, diese mit den Statistiken der Deutschen Bundesbank zu verknüpfen. Soweit die „Gewinnung statistischer Informationen ohne zusätzliche Erhebungen" durch eine Zusammenführung möglich ist, können identische Merkmalsträger in unterschiedlichen Wirtschafts- und Umweltstatistiken über direkte Identifikatoren zusammengeführt werden (record linkage). Dies gilt aber nur für die Wirtschafts- und Umweltstatistiken.

8 Eine Übersicht über die Gesetze, die bei Erhebungen an Schulen zu beachten sind, findet sich bei: Verbund Forschungsdaten Bildung (2015b).

3.6 Europäischer Rechtsrahmen: Ausblick

1995 wurde von der Europäischen Gemeinschaft die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr verabschiedet, um den Datenschutz in Europa zu harmonisieren. Allerdings haben europäische Richtlinien keine unmittelbar verbindliche Wirkung und müssen zunächst in nationale Gesetze umgesetzt werden. Die Datenschutzrichtlinie wurde in Deutschland 2001 durch Anpassung nationaler Vorschriften umgesetzt.

Ab dem 25. Mai 2018 wird die EU-Datenschutzgrundverordnung (EU-DSGVO) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 unmittelbar geltendes Recht in allen Mitgliedsstaaten der Europäischen Union sein. Die EU-DSGVO verfolgt drei Ziele: (a) individuelle Datenschutzrechte sollen besser durchsetzbar werden, (b) es soll für alle europäischen Länder ein einheitliches, harmonisiertes Datenschutzrecht gelten und (c) technischer Datenschutz soll die Datengenerierung reduzieren (vgl. Albrecht 2015). Dies macht eine Anpassung der deutschen Gesetze erforderlich (vgl. Schaar 2016).

Die EU-DGSVO enthält zudem für den öffentlichen Bereich zahlreiche „Öffnungsklauseln", die es den jeweiligen nationalen Gesetzgebern erlauben, eigene (insbesondere ergänzende) Regelungen zu erlassen, die allerdings dem Wesensgehalt der Regelungen der EU-DSGVO nicht zuwiderlaufen dürfen. Beispiele sind etwa (a) die Verarbeitung genetischer, biometrischer oder Gesundheitsdaten (Art. 9 Abs. 4 EU-DSGVO) oder (b) die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken (Art. 89 i. V. m. Art. 5 Abs. 1b EU-DSGVO). Es bleibt abzuwarten, in welchem Umfang und in welcher Ausformung der nationale Gesetzgeber von der Öffnungsklausel Gebrauch macht.

Grundsätzlich bleiben mit der EU-DSGVO wesentliche Grundzüge des Datenschutzrechts unangetastet, so auch das Verbot mit Erlaubnisvorbehalt, das Prinzip der Datenvermeidung, das Prinzip der Datensparsamkeit und das Prinzip der Zweckbindung. Explizit eingeführt werden zudem u. a. das Prinzip der Gewährleistung von Datensicherheit sowie das Recht der Betroffenen auf „Vergessenwerden" (Art. 17 Abs. 2 EU-DSGVO). Eine völlige „Neuauflage" des Datenschutzes ist mit dem Wirksamwerden der EU-DSGVO daher nicht verbunden (weitere Details finden sich bei BfDI 2016b).

4 Grundbegriffe des Datenschutzes für die Forschung

Dieser Abschnitt stellt zentrale Grundbegriffe des Datenschutzes in Deutschland vor, die insbesondere auch empirisch Forschenden im Rahmen ihrer Forschung häufig begegnen.

4.1 Personenbezogene Daten

Personenbezogene Daten sind „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)." (§ 3 Abs. 1 BDSG).

Damit sind alle Informationen umfasst, die über eine Person etwas aussagen. Diese Informationen müssen nicht zwingend eine Person identifizieren, wie bspw. Namen oder ein Foto des bzw. der Betroffenen. Ausreichend ist vielmehr, dass zu der jeweiligen Person ein Bezug hergestellt werden kann. So können, zumindest bei entsprechendem Zusatzwissen, auch Telefon-, Matrikel-, Sozialversicherungsnummern, persönlich zugeteilte Berechtigungskennzeichen und IP-Adressen ein personenbezogenes Datum darstellen und damit datenschutzrelevante Informationen sein. Sofern personenbezogene Daten erhoben, verarbeitet und genutzt werden, muss das Regelwerk des Datenschutzes beachtet werden.

Der Geltungsbereich der Datenschutzgesetze bezieht sich zunächst auf Daten „natürlicher Personen", d. h. auf alle Menschen als Träger von Rechten und Pflichten. Zunehmend finden die Regelungen der Datenschutzgesetze allerdings auch Anwendung auf Informationen, die zunächst „juristische Personen" (d. h. Personenvereinigungen oder Vermögensmassen, die aufgrund gesetzlicher Anerkennung rechtsfähig sind) betreffen. Diese fallen unter den Datenschutz, sofern sie indirekte Angaben über natürliche Personen enthalten, d. h. immer dann, wenn Informationen einer juristischen Person auf eine natürliche Person „durchschlagen". Dies ist möglich bei Daten, die sowohl Informationen auf der Organisations- als auch auf der Individualebene enthalten, beispielsweise bei Personen-Betriebs-Daten oder Daten der Schulforschung mit Informationen zu Lehrenden, Schülern oder Schülerinnen und Schulen. Individuen sind vergleichsweise leichter zu identifizieren, sobald die Organisationen, denen sie angehören, identifiziert sind.

4.2 Sensible personenbezogene Daten

Über den grundsätzlichen Schutz personenbezogener Daten hinaus sehen die Datenschutzgesetze für sensible Daten (d. h. Daten, die spezifische Risiken für Betroffene bergen) einen besonderen Schutz vor. Diese Daten werden als *besondere Arten personenbezogener Daten* (§ 3 Abs. 9 BDSG) bezeichnet. Unter diese Gruppe von Daten fallen:

- ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Angaben zur Gesundheit
- Angaben zum Sexualleben

Die Erhebung, Verarbeitung und Nutzung dieser Datenarten unterliegen höheren Anforderungen. U. a. müssen sich bei auf Einwilligung der Betroffenen basierenden Datenerhebungen bereits die Einwilligungserklärungen ausdrücklich auf diese Daten beziehen.

4.3 Anonymisieren

Anonymisieren bezeichnet 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 (vgl. § 3 Abs. 6 BDSG).

Das Datenschutzrecht unterscheidet damit im Kern zwei Anonymisierungsvarianten: (a) Daten können nicht mehr einer natürlichen Person zugeordnet werden und (b) Daten können nur mit unverhältnismäßig großem Aufwand einer natürlichen Person zugeordnet werden. Beide Varianten gelten als wirksam anonymisiert, sodass solche Daten nicht mehr personenbezogen sind und nicht mehr in den Geltungsbereich des BDSG bzw. der LDSG fallen.

Für die Anonymisierung kommen unterschiedliche Methoden in Betracht. Am relevantesten sind die Methoden zur Veränderung und Reduktion des Informationsgehalts der Daten selbst, wie z. B. Löschung der Identifikationsmerkmale, Merkmalsaggregation oder Maskierungen. Für die Einstufung, ob bzw. nach welcher Methode die Daten als hinreichend anonymisiert gelten, sind regelmäßig aber auch andere Faktoren zu bewerten. Anonymität resultiert also nicht zwingend allein aus dem realen Informationsgehalt der Daten selbst, sondern auch aus den bestehenden Möglichkeiten zur De-Anonymisierung. Wann ein Mikrodatensatz als anonym bezeichnet werden kann, hängt daher u. a. auch davon ab, unter welchen Rahmenbedingungen er verarbeitet bzw. genutzt wird und welches Zusatzwissen vorliegt. Insbesondere die zweite Variante der Anonymisierung kann somit auch durch zusätzliche technisch-organisatorische Maßnahmen des Datenzugangs oder vertragliche Begrenzungen der Datenverarbeitung erreicht werden.

Für beide Varianten der Anonymität fällt es aufgrund des technischen Fortschritts und der online frei zugänglichen Zusatzinformationen zunehmend schwerer zu bestimmen, ob die Anforderungen erfüllt sind (vgl. Schaar 2009). Abhängig davon, wer die Mikrodaten nutzt und unter welchen Rahmenbedingungen die Nutzung stattfindet, kann die Anonymität mit mehr oder minder starken Informationseinbußen oder entsprechenden vertraglichen Regelungen erreicht werden. Forschungsdatenzentren machen Daten daher häufig nur unter kontrollierten Bedingungen auf Basis von Verträgen, die Datennutzer und Datennutzerinnen zur Unterlassung von Re-Identifizierungsversuchen verpflichten, verfügbar.

Bezüglich unterschiedlicher Anonymisierungsvarianten für Forschungsdaten haben sich weitere Begriffe entwickelt, die im Folgenden näher vorgestellt werden.

Absolute Anonymisierung
Die stärkste Form der Anonymisierung von Daten wird als absolute Anonymisierung bezeichnet und entspricht der ersten Anonymisierungsvariante nach § 3 Abs. 6 BDSG. Hierbei sind die Angaben durch Aggregation bzw. Verfremdung oder Schwärzen bzw. Löschen von Daten so verändert, dass eine Zuordnung der Informationen zu den Personen, die diese Angaben gemacht haben, nach aktuellen technischen Möglichkeiten unmöglich wird. Dies gilt beispielsweise für aggregierte Daten, Tabellen oder andere statistische Auswertungen. Daneben können auch die Einzelangaben (Mikrodaten) selbst absolut anonymisiert werden. Durch Stichprobenziehungen, Aggregationen, die Entfernung von Informationen, insbesondere bei qualitativen Daten, oder die Anwendung weiterer Verfahren, können die Daten dabei so stark vergröbert oder verfremdet werden, dass nach menschlichem Ermessen keine Zuordnung der Mikrodaten zu den ursprünglichen Merkmalsträgern mehr möglich ist. Der Informationsgehalt absolut anonymer Mikrodaten ist jedoch stark gemindert, was eine Reduktion der Nutzbarkeit für die Wissenschaft als Quelle tiefergehender Forschungsvorhaben mit sich bringt.

Faktische Anonymisierung
Mikrodaten werden als faktisch anonym bezeichnet, wenn ein Personenbezug nur mit unverhältnismäßig hohem Aufwand wiederhergestellt werden kann. Die in § 3 Abs. 6 BDSG zugrunde gelegte Definition dieser zweiten Anonymisierungsvariante ist hierbei im Wesentlichen deckungsgleich mit der des Bundesstatistikgesetzes (§ 16 Abs. 6 BStatG). Die Hauptzielrichtung der faktischen Anonymisierung besteht darin, durch behutsame Informationsreduktion und Informationsveränderungen die Zuordnungsmöglichkeiten von Merkmalsausprägungen zu den entsprechenden Merkmalsträgern zu verringern, dabei jedoch den analytischen Gehalt der Daten weitgehend zu erhalten. Zur Erreichung einer angemessenen Anonymisierung müssen für jeden einzelnen Datensatz der für einen potentiellen Angreifer erforderliche Aufwand und der vorstellbare Nutzen einer De-Anonymisierung analysiert werden.

Formale Anonymisierung
Der geringste Grad an Anonymisierung ist bei formal anonymisierten Daten gegeben. Die formale Anonymisierung beinhaltet lediglich die Entfernung der direkten Identifikatoren. Hierzu zählen beispielsweise Namen oder Adressen. Der Merkmalsumfang und die fachlichen und regionalen Gliederungen bleiben dagegen erhalten. Die formale Anonymisierung ist bei sozialwissenschaftlichen Daten häufig nicht ausreichend, um die Möglichkeit einer Identifikation der Betroffenen auszuschließen. Ist ein Personenbezug jedoch weiterhin herstellbar, sind die Daten aus datenschutzrechtlicher Sicht nicht anonymisiert.

4.4 Pseudonymisieren

„Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren" (§ 3 Abs. 6a BDSG). Da eine Zusammenführung von Person und Daten grundsätzlich noch möglich bleibt, handelt es sich bei pseudonymisierten Daten grundsätzlich auch noch um personenbezogene Daten.

Bei der Pseudonymisierung werden die direkten Identifikatoren nicht dauerhaft entfernt. An ihre Stelle tritt vielmehr eine (neue) Zahlen- oder Buchstabenkombination, die in der Regel über einen bestimmten Schlüssel vergeben wird. Im Nachhinein kann über die entsprechende Schlüsselbrücke eine De-Anonymisierung der Personen erfolgen. Dabei wird unterschieden zwischen „sprechenden" und „nichtsprechenden" Pseudonymen; erstere bewahren einen vergleichbaren Sinngehalt (z. B. Ersatz eines weiblichen Vornamens durch einen anderen) und erhalten dadurch mehr Analysepotential.

Insbesondere mit Blick auf eine nachhaltige Nutzung auch qualitativer Daten erscheint die Pseudonymisierung als ein geeignetes Verfahren. Die direkten und anderen Identifikationsmerkmale werden dabei im Sinne der wissenschaftlichen Nützlichkeit durch gleichwertige Begriffe bzw. Umschreibungen ersetzt (vgl. Gebel et al. 2015 oder Meyermann und Porzelt 2014).

In besonderen Forschungskonstellationen kann es bei der Nutzung pseudonymisierter Daten hilfreich sein, die Schlüsselbrücke bei einer sog. Vertrauensstelle (Datentreuhänder) aufzubewahren. So haben die Forschenden keine direkte Möglichkeit, Rückschlüsse auf einzelne Personen zu ziehen. Sollten allerdings im Laufe des Forschungsprojektes Fragen oder Unplausibilitäten auftreten, können diese unter Umständen unter Rückgriff auf die Informationen bei der Vertrauensstelle geklärt werden. Zudem eröffnet sich für die wissenschaftliche Sekundäranalyse die Möglichkeit, je nach Forschungsinteresse unterschiedliche Anonymisierungsalternativen verfügbar machen zu können.

4.5 Datenerhebung, -verarbeitung und -nutzung

Nach § 3 Abs. 3 BDSG bezeichnet Erhebung das Beschaffen von Daten über den Betroffenen. Der gesetzliche *Datenverarbeitungsbegriff* umfasst fünf Varianten, die im § 3 BDSG definiert werden: „Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten". Daten*nutzung* ist nach § 3 Abs. 5 BDSG jede Verwendung der Daten, soweit es sich nicht um eine Datenverarbeitung handelt (z. B. das Anschauen der Daten).

4.6 Verantwortliche Stelle

„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." (§ 3 BDSG). Dies ist jede natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Die Festlegung und Benennung der verantwortlichen Stelle bereits im Rahmen der informierten Einwilligung oder in einem Datenschutzkonzept ist wichtig, da diese erster Ansprechpartner für die Betroffenen ist und diese Stelle z. B. bei Verstößen gegen das BDSG nach § 7 BDSG auch für Fragen des Schadenersatzes heranzuziehen ist. In der wissenschaftlichen Forschungspraxis sind dies häufig die Organisationseinheiten, die Forschende beschäftigen (z. B. Hochschulen oder Forschungseinrichtungen).

Erhebt ein Umfrageinstitut im Auftrag einer Forschungseinrichtung Daten, so ist die verantwortliche Stelle zu klären. Gegebenenfalls muss ein Auftragsdatenverarbeitungsvertrag geschlossen werden. Die Bestimmung der verantwortlichen Stelle ist insbesondere deshalb relevant, weil danach die zuständige Aufsichtsbehörde (z. B. Bundes- oder Landesdatenschutzbeauftragte) festgelegt wird.

Vorgaben zu Auftragsdatenverarbeitungsverträgen finden sich in § 11 Abs. 2 BDSG. Sofern es in den Landesdatenschutzgesetzen keine entsprechenden Vorgaben gibt, findet diese Norm auch für Institute mit Länderhoheit Anwendung.[9]

4.7 Datentreuhänder

Ein Datentreuhänder ist eine unabhängige Einrichtung (z. B. ein Notar), die sowohl gegenüber der datenbesitzenden Stelle oder den Betroffenen als auch gegenüber den datennutzenden Stellen (Forschende) personell und räumlich klar getrennt sein muss. Insofern auf einen Datentreuhänder zurückgegriffen wird, muss sowohl rechtlich als auch technisch und organisatorisch gewährleistet werden, dass nur der Datentreuhänder einen Personenbezug bei den Daten herstellen kann, die ihm übermittelt worden sind. Der Datentreuhänder anonymisiert/pseudonymisiert die zu verarbeitenden Daten. Jedoch sollten nicht die Daten selbst, sondern lediglich die Merkmale, die einen direkten Personenbezug ermöglichen (direkte Identifikatoren) und die verwendeten Verschlüsselungsalgorithmen beim Datentreuhänder aufbewahrt werden. Die Funktion des Datentreuhänders ist nicht gesetzlich geregelt (vgl. Metschke und Wellbrock 2002, S. 41 ff.).

Ein Datentreuhänder kann beispielsweise eingesetzt werden, um personenbezogene Daten aufzubewahren, die für die Verknüpfung von Daten aus verschiedenen Quellen oder Wellen benötigt werden (vgl. Metschke und Wellbrock 2002, S. 42 f.).

9 Musterverträge finden sich bspw. auf den Internetseiten des Landesbeauftragten für den Datenschutz in Bayern, ebenso in NRW sowie der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

4.8 Technische und organisatorische Maßnahmen

Alle Stellen, die gem. § 9 BDSG personenbezogene Daten erheben, verarbeiten oder nutzen, sind verpflichtet, technische und organisatorische Maßnahmen (TOM) zu treffen, damit die Sicherheits- und Schutzanforderungen des BDSG erfüllt sind. Die Spezifizierung dieser Anforderungen ergibt sich aus der Anlage zu § 9 Satz 1 BDSG. Dazu gehören beispielsweise die Kontrolle von Zugriff, Weitergabe und Eingabe sowie das Trennungsgebot, d. h. Daten, die zu unterschiedlichen Zwecken erhoben wurden, müssen getrennt verarbeitet werden. Um das Trennungsgebot zu realisieren, sind eine physische und eine organisatorische Trennung sinnvoll.

4.9 Verfahrensverzeichnis

Ein Element des Datenschutzes in Einrichtungen ist das Verfahrensverzeichnis. Es dient der Bestandsaufnahme über die laufenden Arbeiten mit personenbezogenen Daten. Im BDSG findet sich der Begriff selbst nicht. Das Gesetz spricht in § 4g Abs. 2 von einer „Übersicht" die dem betrieblichen Datenschutzbeauftragten zur Verfügung gestellt wird. In der Praxis wird zwischen dem internen und dem öffentlichen Verfahrensverzeichnis unterschieden. Das interne Verzeichnis (auch Verfahrensbeschreibung genannt) ist umfangreicher und dient der betriebsinternen Selbstkontrolle. Das öffentliche Verfahrensverzeichnis (sogenanntes Jedermann-Verzeichnis) muss unter bestimmten Voraussetzungen jeder Person zugänglich gemacht werden und soll die Datenverarbeitungsvorgänge nach außen transparent machen.[10]

10 Ein Beispiel findet sich hier: www.gdd.de/downloads/materialien/muster/verfahrensverzeichnis.pdf.

5 Datenschutzrechtliche Aspekte bei der Feldarbeit

Die folgenden Ausführungen beziehen sich auf Primärdatenerhebungen („Eigenerhebungen"). Bevor für ein Forschungsvorhaben Daten neu erhoben werden, ist zu prüfen, ob der Forschungszweck nicht auch durch die Sekundärauswertung bereits erhobener (anonymisierter) Daten erreicht werden kann (Erforderlichkeitsgrundsatz) (vgl. Häder 2009, S. 9). Dazu ist es zunächst nötig, das Forschungsziel präzise zu bestimmen. Ist eine Nutzung vorhandener Daten nicht möglich, ist bei der Konzeption des Forschungsprojekts auf Datengeeignetheit, Datensparsamkeit, Datenvermeidung und die Wahl des mildesten Mittels zu achten (vgl. Kapitel 2.3). Die zeitliche (und ggf. emotionale) Belastung der Betroffenen sollte so gering wie möglich gehalten werden. Dies gilt in besonderem Maß für sensible, besondere Arten personenbezogener Daten (vgl. § 3 Abs. 9 BDSG und Kapitel 4.2 dieses Papiers). Als wesentlicher Grundsatz gilt, dass personenbezogene Daten nur mit informierter Einwilligung der Betroffenen oder auf Basis einer anderen Rechtsgrundlage erhoben werden dürfen.

Grundsätzlich ist es ratsam, frühestmöglich und bereits bei der Ausgestaltung des Forschungsprojektes Datenschutzbeauftragte einzubeziehen, sofern personenbezogene Daten erhoben werden sollen. Die frühzeitige Erstellung von Forschungsdatenmanagementplänen unterstützt darüber hinaus den Umgang mit personenbezogenen Daten während des gesamten Data-Life-Cycles (vgl. hierzu RatSWD 2016).

5.1 Erhebung und Verarbeitung personenbezogener Daten auf der Grundlage einer Einwilligung der Betroffenen

5.1.1 Anforderungen an die informierte Einwilligung als Grundlage einer Erhebung

Die datenschutzrechtlichen Regelungen legen bestimmte inhaltliche und formale Anforderungen an die Einwilligung fest, mit der „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen" (Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983) ausgeübt wird.

Nach § 4a BDSG ist die rechtzeitige und umfassende Information über die beabsichtigte Nutzung der Daten Grundlage für eine wirksame Einwilligung. Nicht ausreichend informierte Betroffene können nicht wirksam einwilligen, eine Nutzung der Daten wäre in diesem Fall nicht zulässig. Damit die Information über die Datenerhebung für die Betroffenen verständlich ist, sollte die Information laienverständlich verfasst sein; des Weiteren ist die Freiwilligkeit der Einwilligung eindeutig hervorzuheben.

Konkret bedeutet dies, dass den Betroffenen vor der Einwilligung verständliche und vollständige Informationen zu folgenden Fragen vorliegen müssen: „Wer ist der verantwortliche Träger und Leiter des Forschungsvorhabens?", „Durch wen und wie werden die Daten verarbeitet?", „Wozu werden die Daten verarbeitet?", „Welche Daten werden verarbeitet?", „Welcher Personenkreis (einschließlich Kooperationspartner) erhält von den personenbezogenen Daten Kenntnis?" „Wie lange werden die personenbezogenen Daten gespeichert?" (vgl. Metschke und Wellbrock 2002, S. 26).

Wenn eine Wiederholungsbefragung geplant ist, sollten die Betroffenen ebenfalls darüber informiert werden. Damit sie erneut kontaktiert werden können, muss eine Einwilligung zur Speicherung ihrer Kontaktdaten für diesen Zweck eingeholt werden. Mit dieser Einwilligung (Speicherung der Kontaktdaten für eine erneute Einladung) ist keine Einwilligung in eine erneute Studienteilnahme verbunden. Je nach konkretem Forschungsprojekt kann es sich hier empfehlen, diese Einwilligung in einer separaten Einwilligungserklärung abzufragen, sodass Betroffenenrechte ebenfalls getrennt ausgeübt werden können.

Sollen in einem sogenannten „record linkage“ Verfahren, also mittels Verknüpfung verschiedener Datenquellen zu ein und derselben Person, neue Daten angespielt werden, ist dafür eine gesonderte Einwilligungserklärung der Betroffenen erforderlich. Beispiele für Mustereinwilligungserklärungen finden sich u. a. bei Liebig (2014), Metschke und Wellbrock (2002, S. 48 ff.), Verbund Forschungsdaten Bildung (2015a) oder auf den Webseiten des ADM (Arbeitskreis deutscher Markt- und Sozialforschungsinstitute) e. V.

Grundsätzlich muss die Einwilligung schriftlich erfolgen. Ausnahmen von der Regel der Schriftlichkeit sieht das BDSG unter § 4a vor: „Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.“ Bei wissenschaftlicher Forschung liegt ein besonderer Umstand beispielsweise dann vor, wenn durch die Schriftform der Forschungszweck erheblich beeinträchtigt wird oder die schriftliche Einwilligung nur mit einem unverhältnismäßig hohen Aufwand eingeholt werden kann (vgl. Häder 2009, S. 14). Dieses Abweichen von der Schriftlichkeit, dessen Gründe schriftlich zu dokumentieren sind, kann bei telefonischen Erhebungen, die über Telefonstichproben erfolgen, bei Onlinebefragungen, bei ad hoc geführten persönlichen Interviews oder bei besonders sensiblen Forschungsfeldern (bspw. abweichendes Verhalten) zum Tragen kommen. Grundsätzlich ist beim Abweichen vom Gebot der Schriftlichkeit zu bedenken, dass für spätere Nachprüfungen oder Datennutzungen nur schwer belegt werden kann, welches die Inhalte der ursprünglichen Einwilligung waren (vgl. auch Kapitel 5.3).

5.1.2 Konsequenzen für Feldarbeit und spätere Datennutzung

Die Einwilligungserklärung hat eine rechtlich bindende Wirkung für alle an der Forschung Beteiligten. Sie kann jederzeit von den Betroffenen widerrufen werden. Deren Daten (personenidentifizierende und Erhebungsdaten) sind dann aus dem Datensatz zu löschen. Wenn die Studiendaten allerdings durch die datenverarbeitende Stelle anonymisiert sind, endet die Widerrufsmöglichkeit der Betroffenen in Bezug auf diese, weil es dann nicht mehr möglich ist, ihnen bestimmte Angaben im Datensatz zuzuordnen.

Sollen zu einem späteren Zeitpunkt die Daten zu einem anderen, als dem in der Einwilligungserklärung genannten Zweck ausgewertet werden, muss eine neue Einwilligungserklärung von den Betroffenen eingeholt werden (Ausnahme ist hier der bereits genannte „broad consent“, bei dem die Betroffenen relativ breit späteren Forschungen zustimmen, vgl. Kapitel 2.5). Das Zweckbindungsprinzip erfordert, dass der ursprüngliche Datenzweck in allen Phasen der Datenverwendung beibehalten werden muss. Demnach sollten alle möglichen späteren Datennutzungen und Fragestellungen vor Einholen der Einwilligung antizipiert und Gegenstände der Einwilligung werden. Zu diesem Sachverhalt müssen alle an der Studie beteiligten Forschenden (von Studienverantwortlichen über die Interviewer und Interviewerinnen bis zu Datenauswertenden) im Vorfeld geschult werden.

Hinsichtlich der bindenden Wirkung der Einwilligungserklärung ist darüber hinaus insbesondere bei der Durchführung von Forschungsprojekten im Rahmen von Forschungskooperationen zu beachten, dass diese ebenfalls für die Angaben zu den datenverarbeitenden Einrichtungen und ggf. Personen gilt. Spätere Datenübermittlungen an ursprünglich in der Einwilligungserklärung nicht genannte Einrichtungen sind im Rahmen der Einholung einer erneuten Einwilligungserklärung bei den Betroffenen zulässig, was in der Praxis oftmals nur schwer zu realisieren ist.

Die Einwilligungserklärungen, die in der Regel mit Namen versehen sind, sind strikt getrennt von den Erhebungsunterlagen aufzubewahren. Hierfür sind von den Forschenden geeignete technische und organisatorische Maßnahmen zu ergreifen.

5.2 Datenschutzrechtliche Anforderungen bei der Befragung spezieller Personengruppen

Voraussetzung für die informierte Teilnahme an einer Studie ist die Einwilligungsfähigkeit (vgl. Metschke und Wellbrock 2002, S. 30 f. oder Verbund Forschungsdaten Bildung 2015a). Allgemein wird davon ausgegangen, dass erst Jugendliche ab 14 Jahren über genügend Einsichtsfähigkeit verfügen, Studienziele zu verstehen und in diese selbst einzuwilligen. Gleichwohl besteht auch in diesem Alter das elterliche Erziehungsrecht, das bis zur Volljährigkeit ausgeübt werden kann. Üblicherweise wird die Teilnahme vom Vorliegen sowohl der Einwilligung des Jugendlichen als auch der Erziehungsberechtigten abhängig gemacht, wobei von beiden ein positives Votum vorliegen muss. Eine Verweigerung des Jugendlichen kann nicht durch die Eltern beschnitten werden. Bei Schülerstudien ist es zudem erforderlich, die jeweiligen Schul- und sonstigen Landesgesetze sowie ggf. weitere Rechtsgrundlagen zu prüfen und zu berücksichtigen.

Auch volljährige Personen können je nach aktueller Einsichts-, Urteils- und Verständnisfähigkeit vorübergehend oder dauerhaft nicht einwilligungsfähig sein. Zu bedenken ist in einem solchen Fall auch durch die Forschenden, inwieweit eine Teilnahme einer solchen Person an der Studie sinnvoll ist oder ob ein Proxy-Interview (Stellvertreter-Interview) angeraten erscheint. Grundsätzlich muss bei nicht einwilligungsfähigen minderjährigen oder erwachsenen Personen die Einwilligung des gesetzlichen Vertreters rechtswirksam erteilt sein.

Neben der Einwilligungsfähigkeit ist die Freiwilligkeit der Teilnahme eine wesentliche Voraussetzung der informierten Einwilligung. Sie ist besonders zu beachten, wenn die Studie in einem Rahmen erfolgt, in dem ein „besonderes Gewaltverhältnis“ oder eine besondere Abhängigkeit vorliegt, wie eine Befragung von Schülerinnen und Schülern in Schulen oder von Mitarbeiterinnen und Mitarbeitern in Betrieben. In allen solchen Fällen müssen die Betroffenen eine echte Wahl haben, die Datenerhebung zu verweigern, ohne einen Nachteil zu erleiden. Darauf, dass die Freiwilligkeit nicht beeinträchtigt wird, ist beispielsweise auch bei einer Anreizsetzung, einer sogenannten „Incentivierung“, von Studienteilnehmenden zu achten.

5.3 Besonderheiten der Einwilligung bei unterschiedlichen Erhebungsarten

Bei Studien, die auf einem Stichprobenansatz beruhen, bei dem die Betroffenen vorher bekannt sind (z. B. Einwohnermeldeamtsstichproben) können die Informationsmaterialien und die Einwilligungserklärungen zur Studie rechtzeitig postalisch zusammen mit der Einladung zur Teilnahme versendet werden oder, z. B. im Rahmen von Face-to-Face-Interviews, direkt vor Beginn der Teilnahme mit den Betroffenen durchgegangen werden. In der Regel kann dann die Einwilligungserklärung hier auch schriftlich erfolgen, beispielsweise zusammen mit dem Rückversand eines ausgefüllten Papierfragebogens. Wenn eine schriftliche Einladung erfolgt, die Datenerhebung aber (auch) online über einen gesicherten Link und einen personifizierten Zugang erfolgt, stellt sich die Frage, inwieweit die Rücksendung einer schriftlichen Einwilligungserklärung logistisch sinnvoll ist. Es kann dann die Situation entstehen, dass die Betroffenen zwar an der Befragung teilnehmen, aber keine gültige Einwilligungserklärung vorliegt, sodass der Datensatz gelöscht werden müsste. In diesem Fall ist in Absprache mit den zuständigen Datenschutzbeauftragten zu klären, ob die Einwilligung ebenfalls online, vor Beginn der Befragung, erfolgen kann. Diese kann durch ein aktives „opt-in“ der Betroffenen erfolgen, wobei die Einwilligungserklärung während des Erhebungsprozesses jederzeit von den Betroffenen eingesehen und widerrufen werden kann.

Bei einem Zugang über Telefonstichproben, aktuell meistens sogenannte „Dual-Frame-Stichproben“ mit einer Zufallsauswahl von Mobilfunk- und Festnetznummern, ist eine vorherige Information der Betroffenen in der Regel nicht möglich. Die Einwilligung wird dann – nach mündlicher Information der Interviewer über den Zweck der Studie – in der Regel mündlich erteilt. Dies muss im Erhebungssystem dokumentiert werden. In diesem Fall greift § 4a Abs. 2 BDSG (vgl. Kapitel 5.1).

5.4 Datenverarbeitung und -speicherung während der Feldarbeit

Grundsätzlich gilt bei der Datenverarbeitung und -speicherung während der Feldarbeit ein striktes Trennungsgebot; zudem sollten Merkmale, welche die persönliche Identifizierung ermöglichen (Identifikatoren) so früh wie möglich gelöscht bzw. vom Erhebungsdatensatz getrennt werden. Bei der eigentlichen Datenerhebung ist das strikte Trennungsgebot aber faktisch nicht immer möglich, zum Beispiel dann, wenn Interviewerinnen und Interviewer bei Face-to-Face-Interviews direkt die Angaben der Betroffenen erfassen. Daher müssen am Forschungsprozess Beteiligte, die Kenntnis persönlicher Angaben erhalten können, über die Erforderlichkeit der Geheimhaltung aufgeklärt und entsprechend verpflichtet werden.

Technisch lassen sich durch getrennte Datenbanksysteme für personenidentifizierende Daten (Adressdaten etc.) sowie für die Erhebungsdaten ungewollte Zusammenführungen der Daten so weit wie möglich vermeiden. Bei Querschnittserhebungen, für die eine nochmalige Kontaktaufnahme zu den Betroffenen nicht vorgesehen ist, können die personenidentifizierenden Merkmale unmittelbar mit dem Feldende bzw. dann, wenn ein Fall abgeschlossen ist (also ein endgültiges Ergebnis, ob bei einer bestimmten Person Daten erhoben werden konnten oder nicht, vorliegt), gelöscht werden. Bei Längsschnittdaten oder bei registerbasierten Daten, über die Verläufe abgebildet werden sollen, müssen Schlüssel bzw. nicht-sprechende Identifikatoren verwendet werden. In diesem Fall gilt das Gebot der frühestmöglichen Pseudonymisierung der Daten.

Mit dem Rückgriff auf Datentreuhänder (oder Vertrauensstellen, vgl. Kapitel 4.7) kann der Schutz der personenbezogenen Daten gewährleistet werden, ohne dass der Datenzugang der Forschung behindert wird. Der Datentreuhänder übernimmt die Rolle eines vertrauenswürdigen Dritten und bewahrt zum Bespiel die personenidentifizierenden Daten oder die Schlüssel zum Zusammenführen auf. Datentreuhänder können eigenständige Personen oder Einrichtungen sein, die von den Forschenden räumlich und personell klar getrennt sind. Eine Möglichkeit ist, bestehende Forschungsdatenzentren als „Ort des Datenschutzes“ zu nutzen. Die Aufgabe kann alternativ von den unabhängigen Datenschutzbeauftragten einer Einrichtung wahrgenommen werden. Bei Längsschnittstudien können die Identifizierungsmerkmale beim Datentreuhänder verbleiben, sodass zu späteren Zeitpunkten beim Treuhänder, nicht aber bei der forschenden Stelle erneut personenbezogene Zuordnungen mit neuen Daten vorgenommen werden können. Da Daten zunehmend nicht mehr in Papierform oder auf separaten Datenträgern gespeichert werden, kann auch ein völlig getrenntes IT-System, welches keinerlei Zusammenführung erlaubt, und bei dem nur der Datentreuhänder Zugriff auf die Identifikatoren hat, an Stelle einer räumlichen Trennung treten.

Neben den bereits erwähnten personenidentifizierenden Daten und den eigentlichen Erhebungs- oder Befragungsdaten fallen während des Erhebungsprozesses noch weitere Daten an. Diese betreffen zum Beispiel die Art und Anzahl der Kontaktierungen, die Dauer der Beantwortung einzelner Fragen (bei computerassistierten Datenerhebungssystemen) oder Informationen zum Verhalten von Interviewer und Interviewerinnen. Mit der Zunahme computerassistierter Erhebungsformen (CATI, CAPI, CAWI) steigt auch die Menge im Erhebungsprozess anfallender Daten, sogenannter Paradaten (vgl. Kreuter und Casas-Cordero 2010). Diese Daten können zur Qualitätssicherung der Studie eingesetzt werden. Gleichwohl sind die rechtlichen und ethischen Aspekte bei der Verwendung noch weitgehend ungeklärt. Unterschieden werden sogenannte Prozess-Paradaten (process paradata), die beim Erhebungsprozess anfallen und Zusatzdaten (auxiliary paradata), z. B. Beobachtungen der Interviewerinnen und Interviewer und oder zusätzliche Informationen zu den Betroffenen oder auch Feldnotizen und Interviewprotokolle im Rahmen qualitativer Erhebungen. Es ist auch für diese Daten zu bedenken, ob sie genutzt werden sollen, inwieweit für ihre Verwendung eine Einwilligung erforderlich ist und wie die Vertraulichkeit gewährleistet werden kann (beispielsweise durch frühzeitige Entfernung von Identifikatoren oder anderen Merkmalen, die eine Re-Identifizierung ermöglichen könnten) (vgl. Schmidutz und Bristle 2013).

Für alle während der Feldarbeit anfallenden Daten gilt, dass die Datenflüsse im Vorfeld in einem Datenmanagementplan genau zu definieren sind, entsprechende datenbanktechnische und methodische Vorkehrungen getroffen werden müssen und eine möglichst nahtlose Dokumentation des Erhebungsprozesses erfolgen sollte (RatSWD 2016).

5.5 Umgang mit Verweigerungen, Widerruf von Einwilligungen, Sperrung und Löschung von Daten

Aufgrund der Freiwilligkeit der Teilnahme, auf die ausdrücklich hinzuweisen ist, ist niemand, der zur Teilnahme an einer Studie eingeladen wird, verpflichtet sich zu beteiligen (Ausnahmen sind Erhebungen mit gesetzlicher Auskunftspflicht, wie z. B. der Mikrozensus). Den Betroffenen, die die Teilnahme verweigern, dürfen weder Nachteile entstehen, noch darf Druck zur Teilnahme ausgeübt werden. Eine Verweigerung ist unmittelbar zu akzeptieren. Insbesondere bei telefonischen Erhebungen werden nochmalige Anrufversuche, z. B. durch einen anderen Interviewenden, als kritisch angesehen (vgl. Häder 2009, S. 15).

Betroffene haben jederzeit das Recht, die Einwilligung zur Teilnahme und Verarbeitung ihrer Daten zu widerrufen. Ihnen steht darüber hinaus das Recht auf Auskunft über die die eigene Person betreffenden Daten sowie das Recht auf Berichtigung fehlerhafter Daten zu. Wenn ein Widerruf seitens eines Betroffenen erfolgt, sind – sofern das technisch noch möglich ist – sämtliche Daten, die auf Grundlage der Einwilligung erhoben wurden, inklusive der dazugehörenden personenbezogenen Prozessdaten (wie z. B. Daten zu den Kontaktversuchen) zu löschen bzw. zu sperren (dies trifft auch auf pseudonymisierte Daten zu[11]; bei anonymen Daten ist es nicht mehr möglich, einen einzelnen Fall im Datensatz einer einzelnen Person zuzuordnen).

In § 35 Abs. 3 BDSG ist definiert, unter welchen Umständen an Stelle der Löschung eine Sperrung der Daten treten kann. Dies ist u. a. dann der Fall, wenn „einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen“ (z. B. zehn Jahre, wie es in diversen Regeln guter wissenschaftlicher Praxis, die satzungs- oder vertragsmäßigen Charakter haben, definiert wird) oder wenn „eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist“ (ebd.). Dies kann z. B. bei in Back-up-Systemen gespeicherten Daten der Fall sein (was im Einzelfall jedoch zu überprüfen ist). Die Lösch- bzw. Sperrpflichten finden grundsätzlich ebenfalls auf alle personenidentifizierenden Daten, wie Adress- oder Kontaktdaten, Anwendung (wenn diese auf Grundlage einer Einwilligung erhoben wurden oder auf dieser weiter verarbeitet werden), es sei denn, dass die Daten auf einer anderen Rechtsgrundlage, wie z. B. dem Bundesmeldegesetz (BMG) erhoben wurden. Sofern Daten gelöscht oder als gesperrt gekennzeichnet werden, ist dies in geeigneter Art und Weise zu dokumentieren.

Grundsätzlich hat ein Widerruf keine Auswirkung auf bereits publizierte, aggregierte Auswertungen. Diese beruhen zudem auf einem Datensatz, der zum Zeitpunkt der Auswertung rechtlich korrekt verarbeitet wurde. Zudem lassen statistische Analysen und abstrahierte Darstellungen qualitativer Ergebnisse keinen Rückschluss auf einzelne Personen zu. Für spätere Auswertungen kann aber nur der bereinigte Datensatz verwendet werden (sofern es sich nicht um in § 35 Abs. 8 BDSG geregelte Fälle handelt, z. B. „zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot“). Dass nur ein bereinigter Datensatz verwendet wird, ist in der datenverarbeitenden Stelle sicherzustellen.

11 Grundsätzlich betrifft die Löschungspflicht bei pseudonymisierten Daten nur die Zuordnungsschlüssel. Ohne diesen sind die Daten anonym und fallen somit nicht mehr unter das Schutzrecht des BDSG. Sofern Betroffene jedoch die Löschung aller ihrer Daten fordern, müssen über die Zuordnungsschlüssel hinaus auch sämtliche Inhalte aus dem Datensatz entfernt werden.

6 Datenschutzrechtliche Aspekte nach der Feldarbeit

6.1 Datenaufbereitung, Datenanalyse: Verarbeitung der Daten nach der Feldphase

Nachdem Daten im Feld erhoben wurden, stellt sich je nach Forschungsprojekt die Frage, wie mit den Kontaktdaten der Teilnehmenden umgegangen werden soll und muss. In einem der Feldphase nahen Zeitabschnitt kann es diesbezüglich noch angemessen und sinnvoll sein, Kontaktdaten aufzubewahren, um möglicherweise auftretende Ungereimtheiten klären zu können; es kann auch, wie bei allen Panelstudien, notwendig sein, diese bis zum Abschluss der letzten Erhebungswelle dauerhaft vorzuhalten. Wenn ein externes Umfrageinstitut mit der Durchführung der Erhebung betraut wurde, kann aus Datenschutzsicht der Vorteil der physischen Trennung genutzt werden, indem die Kontaktdaten der Befragungspersonen beim Institut verbleiben und nur die Befragungsdaten an die Forschungsgruppe übermittelt werden (vgl. z. B. Frick et al. 2010, S. 11). Sollte eine solche strikte Trennung von Beginn an nicht möglich sein, sollten grundsätzlich alle Mitarbeitende, die mit personenbezogenen Daten und pseudonymisierten Daten arbeiten, auf Geheimhaltung bzw. Einhaltung der Datenschutzbestimmungen verpflichtet werden. Hier ist u. a. auch an studentische Hilfskräfte oder Mitarbeitende in Sekretariaten zu denken.

Die Forschungseinrichtungen, die personenbezogene Daten verarbeiten, sind dazu verpflichtet, technische und organisatorische Maßnahmen zu treffen, die die Sicherheits- und Schutzanforderungen des BDSG gewährleisten (vgl. § 9 BDSG und Kapitel 4.8). Insbesondere bedeutet dies auch sicherzustellen, dass kein Unberechtigter auf die Daten zugreifen kann und entsprechende Zugangs- und Zugriffskontrollen eingerichtet sind.

Nach der Datenerhebung gilt es, die Daten schnellstmöglich zu anonymisieren bzw. zu pseudonymisieren. Von einer Anonymisierung sollte nur dann abgesehen werden, wenn der Forschungszweck dagegen spricht oder die Anonymisierung nicht möglich ist (z. B. Videodaten). Hinweise zur Anonymisierung quantitativer Daten finden sich u. a. bei Kinder-Kurlanda und Watteler (2015) oder Schmidutz et al. (2013), zur Anonymisierung qualitativer Daten beispielsweise bei Meyermann und Porzelt (2014) oder Gebel et al. (2015). Dort finden sich auch Übersichten über Merkmale, die voraussichtlich besonders hohe Re-Identifizierungsrisiken mit sich bringen. Insbesondere ist dabei auf Merkmale zu achten, die, nachdem sie mit anderen Datensätzen verknüpft werden, eine De-Anonymisierung ermöglichen können, wie beispielsweise Geodaten (vgl. Schmidutz et al. 2013, S. 37).

6.2 Datenpublikation: Verwendung von Daten in Publikationen

Bei der Verwendung von Daten in Publikationen ist auf absolute Anonymität zu achten. Grundsätzlich sollte keine Veröffentlichung von Rohdaten erfolgen. Bei qualitativen Daten sollte darüber hinaus bspw. keine Veröffentlichung kompletter Transkripte erfolgen (vgl. z. B. die Nutzungsbedingungen des Forschungsdatenzentrums Qualiservice (eScience lab o. D.)). Bei quantitativen Daten ist auf eine Mindestzellbesetzung in Tabellen zu achten. In § 40 Abs. 3 BDSG werden Ausnahmen geregelt.

6.3 Datenaufbewahrung und -archivierung

Gemäß den Regeln guter wissenschaftlicher Praxis (z. B. DFG 2013) sind Forschungsdaten nach Projektabschluss für mindestens zehn Jahre aufzubewahren. Hinzu kommen Anforderungen von Seiten der Förderer, wie BMBF oder DFG, Forschungsdaten „in weitergabefähiger Form auf Anfrage zur Verfügung zu stellen" (BMBF 2015[12]) oder „so zeitnah wie möglich verfügbar" zu machen (DFG[13]). In seinen Empfehlungen von 2016 schlägt der RatSWD ein dreistufiges Archivierungs- und Zugangsmodell für Forschungsdaten vor:

1. nachhaltige Sicherung von Forschungsdaten bei den Datenproduzenten oder einem Dateninfrastrukturpartner ohne nutzerfreundliche Dokumentation und ohne Nachnutzungsmöglichkeit

2. nachhaltige Sicherung von Forschungsdaten mit nutzerfreundlicher Dokumentation und mit restriktiven Nachnutzungsmöglichkeiten bei den Datenproduzenten oder einem Dateninfrastrukturpartner.

3. nachhaltige Sicherung und Bereitstellung von Forschungsdaten mit nutzerfreundlicher Dokumentation bei einer Dateninfrastruktureinrichtung.

Die jeweils erforderlichen Maßnahmen und Arbeitsschritte müssen frühzeitig eingeplant werden (vgl. RatSWD 2016). Die Erfahrungen von Forschungsdatenzentren zeigen, dass den Anforderungen in vielen Fällen nicht nachgekommen werden kann, da die eingeholten Einwilligungen eine spätere Archivierung der Daten und deren Bereitstellung für Dritte nicht erlauben.[14] Vorzugsweise sollten nichtpersonenbezogene Daten archiviert werden. Sollen jedoch *personenbezogene* Daten archiviert werden, ist daher darauf zu achten, hierfür die erforderliche Einwilligung einzuholen bzw. die Teilnehmenden von vornherein auf satzungsmäßige oder vertragliche Aufbewahrungsfristen hinzuweisen. Des Weiteren können Daten können in bestimmten Ausnahmefällen aufgrund des „Forschungsprivilegs" (§ 14 Abs. 2 Nr. 9 bzw. § 28 Abs. 6 BDSG) archiviert und weitergegeben werden. Das Forschungsprivileg sieht vor, dass Daten auch ohne Einwilligung zu Forschungszwecken verarbeitet werden dürfen, wenn bestimmte Kriterien erfüllt sind.

Bei der Aufbewahrung personenbezogener Daten sind wie auch bei der Erhebung und Verarbeitung solcher Daten angemessene technische und organisatorische Maßnahmen (vgl. § 9 BDSG, vgl. Kapitel 4.8) zu treffen. Dabei ist insbesondere auch das Trennungsgebot zu beachten, wonach Adressdaten auch technisch von Befragungsdaten getrennt aufzubewahren sind. Eine solche Aufbewahrung personenbezogener Daten für einen langen Zeitraum bringt dabei teils hohe Anforderungen mit sich, die in einzelnen Forschungsprojekten über das Projektende hinaus ggf. nur schwer gewährleistet werden können. In solchen Fällen können professionelle Forschungsdatenzentren oder Repositorien mit personenunabhängigen Arbeitsroutinen und der notwendigen technischen Ausstattung die datenschutzrechtskonforme Aufbewahrung der Daten übernehmen. Zudem besteht die Möglichkeit, je nach Sensibilität und Schutzanforderungen der Daten unterschiedliche Zugangsstufen zu vereinbaren, die je nach datenschutzrechtlichen Anforderungen unterschiedliche Archivierungs- und Nutzungsstufen für die Daten ermöglichen bzw. begrenzen (vgl. Kapitel 6.4).

12 Vgl. z. B. https://www.bmbf.de/foerderungen/bekanntmachung.php?B=1003, Zugriff am 16.03.2016.
13 Vgl. http://www.dfg.de/foerderung/antragstellung_begutachtung_entscheidung/antragstellende/ antragstellung/nachnutzung_forschungsdaten, Zugriff am 16.03.2016.
14 Faktisch und absolut anonyme Daten unterliegen nicht mehr dem Datenschutz; hier ist Aufbewahrung insofern unproblematisch.

Insbesondere in der qualitativen Forschung wird befürchtet, dass die Bitte um Zustimmung zur Archivierung das Vertrauensverhältnis zwischen Forschenden und Betroffenen stört und damit einen erheblichen negativen Einfluss auf die Teilnahmebereitschaft haben könnte. Empirische Befunde hierzu sind bislang rar (siehe aber Kuula 2011). Um denkbare negative Auswirkungen auf die Teilnahmebereitschaft auszuschließen, besteht die Möglichkeit, die Einwilligung zur Studienteilnahme getrennt von der Einwilligung zur Archivierung der Forschungsdaten einzuholen.[15] Dabei kann eine Nachnutzung von Forschungsdaten auch im Sinne des Datenschutzes interpretiert werden, insofern sie zur Datensparsamkeit und Datenvermeidung (vgl. § 3a BDSG) beiträgt.

Vor diesem Hintergrund hat sich in der Vergangenheit die Sichtweise von Datenschützern und auch von Ethikkommissionen zur Zweckgebundenheit von Einwilligungserklärungen verändert. Während ursprünglich Einwilligungserklärungen nur dann als wirksam angesehen wurden, wenn sie klar definierte, enge Zweckbestimmungen (informed consent) enthielten, werden mittlerweile (je nach Forschungsprojekt) auch weit gefasste Zweckangaben (broad consent) als ausreichend angesehen. Eine allzu enge Zweckbindung einer Einwilligungserklärung kann dem Fortgang der Forschung hinderlich sein und der Forschungsfreiheit widersprechen. Weit gefasste Zweckbestimmungen in Einwilligungserklärungen können helfen (datenschutztechnisch unerwünschte) Mehrfacherhebungen von vergleichbaren Daten zu vermeiden, indem sie die Mehrfachnutzung einmal erhobener Daten zu mehr als einem Forschungszweck ermöglichen. Weit gefassten Einwilligungserklärungen (z. B. *„Ich willige ein, dass meine personenbezogenen Daten über den Rahmen der beschriebenen Studie hinaus auch Dritten für derzeit noch unbekannte Vorhaben zu Zwecken der Bildungsforschung weitergegeben werden können"*) ist als Korrektiv das Recht der Einwilligenden zur Seite gestellt, ihre Einwilligung (mit Wirkung für die Zukunft) jederzeit ohne Angabe von Gründen widerrufen zu können.

Die Formulierung einer wirksamen Einwilligungserklärung ist anspruchsvoll (vgl. Kapitel 5.1.1). Eine Anforderung besteht darin, dass Betroffene in der Lage sein müssen, die Konsequenzen ihrer Zustimmung absehen zu können. Für den Fall der Langzeitarchivierung von Forschungsdaten, d. h. für Zeiträume von zehn Jahren und länger, ist dies kritisch zu betrachten. Der zukünftige Wandel von Rahmenbedingungen und deren Auswirkungen auf die zum heutigen Zeitpunkt gegebene Zustimmung ist letztlich nicht absehbar. Negative Auswirkungen könnten beispielsweise veränderte Gesetzeslagen oder veränderte politische Konstellationen mit sich bringen. Hier hat die Archivierung auch eine ethische Dimension. Langzeitarchivierungskonzepte sollten berücksichtigen, vormals gegebene Einwilligungen hinsichtlich ihrer aktuellen Gültigkeit zu beurteilen.

6.4 Sekundärdatennutzung

Forschungsdaten werden Wissenschaftlerinnen und Wissenschaftlern über verschiedene Wege zur Sekundärdatennutzung bereitgestellt. Bei der Sekundärnutzung von Daten spielen die vom Rat für Sozial- und Wirtschaftsdaten akkreditierten Forschungsdatenzentren (FDZ) eine unterstützende Rolle.

Bei der Bereitstellung von Sekundärdaten werden folgende Optionen unterschieden: Public Use File (PUF) oder Scientific Use File (SUF), kontrollierte Datenfernverarbeitung (KDFV), Remote Access oder Gastwissenschaftleraufenthalte. Bei Public Use Files handelt es sich um absolut anonyme Daten, bei Scientific Use Files um faktisch anonyme Daten (vgl. auch Kap. 4.3). Während PUFs für die breite Öffentlichkeit verfügbar sind, sind SUFs nur für die Fachöffentlichkeit zu wissenschaftlichen Zwecken zugänglich. Diese Verfahren unterscheiden sich von den Verfahren der KDFV und des Remote Access, denn bei letzteren findet keine Weitergabe der Daten an Sekundärforschende statt.

15 Dieses Vorgehen findet sich beispielsweise in den Muster-Einverständniserklärungen von Qualiservice (www.qualiservice.org/fileadmin/templates/qualiservice/Einverstaendnis2013_08.pdf, Zugriff am 21.03.2016) und von der Arbeitsgruppe Datenschutz und qualitative Sozialforschung (Liebig et al. 2014).

Beim Verfahren der KDFV wird die von Forschenden auf Basis von Testdatensätzen erstellte Syntax an das FDZ übermittelt und ausschließlich durch FDZ-Personal auf Grundlage der Originaldaten verarbeitet. Bei den Testdatensätzen handelt es sich um sog. Datenstrukturfiles, die technisch identisch sind mit den Originaldatensätzen, aber inhaltlich so verändert wurden, dass keine sinnvollen Ergebnisse erstellt werden können. Sekundärforschende erhalten ausschließlich die auf Basis der Originaldaten erstellten Auswertungsdateien (Tabellen und Grafiken), die zuvor von FDZ-Mitarbeitenden auf die Einhaltung der Geheimhaltung geprüft wurden. Zur Sicherstellung der primären und sekundären Geheimhaltung kann es u. a. zum Sperren/Schwärzen von Tabellenfeldern kommen. Beim Remote Access können Forschende vom eigenen Arbeitsplatzrechner die Daten einsehen, es ist ihnen aber nicht möglich, die Daten lokal zu speichern. Der Gastwissenschaftlerarbeitsplatz erlaubt es Forschenden, ausschließlich in den Räumlichkeiten und an den abgeschotteten Arbeitsplätzen des FDZ auf die Daten zuzugreifen. Spezielle IT wird bereitgestellt, sodass es Forschenden nicht möglich ist, Daten zu speichern oder zu übermitteln. Es ist ebenfalls nicht erlaubt, eigene Hardware (z. B. Laptop) mitzuführen. Zusätzlich wird jeder dieser vier Zugangswege durch spezielle Nutzungsbedingungen vertraglich abgesichert, in denen sich Sekundärnutzende gegenüber den FDZ u. a. verpflichten, Re-Identifizierungsversuche zu unterlassen.

Literaturverzeichnis

Albrecht, Jan Philipp (2015) Die Datenschutzreform der Europäischen Union, Brüssel.

BfDI (2005) Handreichung „Datenschutzgerechtes eGovernment“, www.bfdi.bund.de/SharedDocs/Publikationen/PM29-04HandreichungDatenschutzgerechtese Government.html [30.03.2016]

BfDI (2015) 25. Tätigkeitsbericht zum Datenschutz 2013–2014, http://www.bfdi.bund.de/SharedDocs /Publikationen/Taetigkeitsberichte/TB_BfDI/25TB_13_14.pdf?__blob=publicationFile&v=10 [24.10.2016]

BfDI (2016a) Datenschutz-Wiki, https://www.bfdi.bund.de/bfdi_wiki/index.php/Zweckbindung, [29.03.2016]

BfDI (2016b) Datenschutz-Grundverordnung, BfDI-Info 6, Bonn.

BIPS (Leibniz Institut für Präventionsforschung und Epidemiologie) (2016) Memorandum – Gesellschaftlicher Nutzen von Gesundheitsdatenbanken und rechtlicher Regelungsbedarf, mimeo, Bremen.

BMAS (Bundesministerium für Arbeit und Soziales) (2015) Übersicht über das Sozialrecht, 12. Auflage 2015, Nürnberg.

DFG (Deutsche Forschungsgemeinschaft) (2013) Sicherung guter wissenschaftlicher Praxis, verfügbar unter: http://www.dfg.de/download/pdf/dfg_im_profil/reden_stellungnahmen/download/empfehl ung_ wiss_praxis_1310.pdf [17.05.2016]

eScience lab (o.D.) Vereinbarung zur Nutzung von Interviewtranskripten, verfügbar unter: http://www.qualiservice.org/fileadmin/templates/qualiservice/Nutzungsvereinbarung_F.pdf, [30.05.2016]

Frick, Joachim R., Jan Goebel, Hansjörg Haas, Peter Krause, Ingo Sieber, Michaela Engelmann (2010) Verfahren für den Datenschutz beim Zugang zu den SOEP-Daten innerhalb und außerhalb des DIW Berlin. verfügbar unter: https://www.diw.de/documents/dokumentenarchiv/17/diw_01.c.347090.de/soep_datenschutzverfahren.pdf [31.05.2016]

Gebel, Tobias, Matthis Grenzer, Julia Kreusch, Stefan Liebig, Heidi Schuster, Ralf Tscherwinka, Oliver Watteler, Andreas Witzel (2015) Verboten ist, was nicht ausdrücklich erlaubt ist: Datenschutz in qualitativen Interviews, Forum Qualitative Sozialforschung, 16/2, 22 S. URN: urn:nbn:de:0111-dipfdocs-110425

Gerling, Rainer W. (2008) Einwilligung und Datenweitergabe in der Forschung, Datenschutz und Datensicherheit 11, 733–735

Gola, Peter, Christoph Klug, Barbara Körffer, Rudolf Schomerus (2015) §§ 1, 3, 40 Bundesdatenschutzgesetz. In: Bundesdatenschutzgesetz (BDSG) Kommentar. Hrsg. Peter Gola und Rudolf Schomerus. 12. Auflage. München: C.H. Beck Verlag.

Häder, Michael (2009) Der Datenschutz in den Sozialwissenschaften – Anmerkungen zur Praxis sozialwissenschaftlicher Erhebungen und Datenverarbeitung in Deutschland, RatSWD Working Paper Series Nr. 90, Berlin.

Hessischer Datenschutzbeauftragter (2001) Datenschutzrechtliche Regelung zur Forschung mit personenbezogenen Daten. verfügbar unter: https://www.datenschutz.hessen.de/download.php? download_ID=13 [11.08.2016]

Hochfellner, Daniela, Dana Müller, Anja Wurdack (2012a) Biographical Data of Social Insurance Agencies in Germany: Improving the Content of Administrative Data, Schmollers Jahrbuch 132(3), 443–451.

Hochfellner, Daniela, Dana Müller, Alexandra Schmucker, Elisabeth Roß (2012b) Datenschutz am Forschungsdatenzentrum, FDZ-Methodenreport 06/2012, IAB Nürnberg.

Kinder-Kurlanda, Katharina, Oliver Watteler (2015) Hinweise zum Datenschutz – Rechtlicher Rahmen und Maßnahmen zur datenschutzgerechten Archivierung sozialwissenschaftlicher Forschungsdaten. GESIS Papers 2015/01, Technical Report DOI: 10.13140/RG.2.1.3821.2641

Kreuter, Frauke, Carolina Casas-Cordero (2010) Paradata, RatSWD Working Paper Series Nr. 136, Berlin.

Kuula, Arja (2011) Methodological and Ethical Dilemmas of Archiving Qualitative Data. IASSIST Quarterly 35 (1–2), 12–17.

KVI (Kommission zur Verbesserung der informationellen Infrastruktur zwischen Wissenschaft und Statistik) (2001) Wege zu einer besseren informationellen Infrastruktur, Nomos Verlagsgesellschaft, Baden-Baden.

Liebig, Stefan, Tobias Gebel, Matthis Grenzer, Julia Kreusch, Heidi Schuster, Ralf Tscherwinka, Oliver Watteler, Andreas Witzel (2014) Anforderungen bei der Generierung und Archivierung qualitativer Interviewdaten. RatSWD Arbeitsgruppe Datenschutz und Qualitative Sozialforschung, RatSWD Working Paper Series Nr. 238, Berlin.

Metschke, Rainer, Rita Wellbrock (2002) Datenschutz in Wissenschaft und Forschung, Materialien zum Datenschutz Nr. 28, verfügbar unter: www.datenschutz-berlin.de/attachments/47/Materialien28.pdf [7.10.2015]

Meyermann, Alexia, Maike Porzelt (2014) Hinweise zur Anonymisierung von qualitativen Daten. forschungsdaten bildung informiert, Nr. 1. Frankfurt am Main: Deutsches Institut für Internationale Pädagogische Forschung, verfügbar unter: www.forschungsdaten-bildung.de/fdb-informiert [30.05.2016]

RatSWD (Rat für Sozial- und Wirtschaftsdaten) (2016) Output 3 – Forschungsdatenmanagement in den Sozial-, Verhaltens- und Wirtschaftswissenschaften. Orientierungshilfen für die Beantragung und Begutachtung datengenerierender und datennutzender Forschungsprojekte, verfügbar unter http://www.ratswd.de/publikationen/output [13.09.2016]

Schaar, Katrin (2016) Was hat die Wissenschaft beim Datenschutz künftig zu beachten? Allgemeine und spezifische Änderungen beim Datenschutz im Wissenschaftsbereich durch die neue Europäische Datenschutzgrundverordnung, RatSWD Working Paper Series Nr. 275, Berlin.

Schaar, Peter (2009) Data protection and statistics – a dynamic and tension-filled relationship. RatSWD Working Paper Series No 82, Berlin.

Schmidutz, Daniel, Johanna Bristle (2013) Paradata: Ethical and Legal Issues, Deliverable D6.2 of Data Service Infrastructure for the Social Sciences and Humanities (DASISH), verfügbar unter: http://dasish.eu/publications/projectreports/D6.2_Paradata.pdf [30.05.2016]

Schmidutz, Daniel, Lorna Ryan, Anje Müller Gjesdal, Koenraad De Smedt (2013) Report about New IPR Challenges: Identifying Ethics and Legal Challenges of SSH Research. Deliverable D6.1 of Data Service Infrastructure for the Social Sciences and Humanities (DASISH), verfügbar unter: http://dasish.eu/deliverables/ [30.05.2016]

Sheehan, Mark (2011) Can Broad Consent be Informed Consent? Public Health Ethics 4(3), 226–235

Verbund Forschungsdaten Bildung (2015 a) Checkliste zur Erstellung rechtskonformer Einwilligungserklärungen mit besonderer Berücksichtigung von Erhebungen an Schulen, verfügbar unter: http://www.forschungsdaten-bildung.de/files/FDB_Einwilligung_Checkliste.pdf [18.05.2016]

Verbund Forschungsdaten Bildung (2015 b) Übersicht über die länderspezifischen Besonderheiten für Befragungen an Schulen, verfügbar unter: http://www.forschungsdaten-bildung.de/genehmigungen [11.08.2016]

Anhang

Übersicht über die Rechtsgrundlagen der Datenbereitstellung in den akkreditierten Forschungsdatenzentren

DATENZENTRUM	BDSG	LDSG	SGB	BStatG	KWG	EU VO	UrhG	UWG	Sonst.
Archiv für Gesprochenes Deutsch (AGD)	x	x							
Allgemeine Bevölkerungsumfrage der Sozialwissenschaften (ALLBUS)	x								
Bundesinstitut für Berufsbildung (BIBB)	x								
Bundesbank	x			x	x	x			x
Bundeszentrale für gesundheitliche Aufklärung (BZgA)	x								
Deutsches Institut für Internationale Pädagogische Forschung (DIPF)	x	x					x		
Deutsches Jugendinstitut (DJI)	x								
Deutsche Rentenversicherung Bund			x						
Betriebs- und Organisationsdaten (BO)	x	x							
Deutsches Zentrum für Altersfragen (DZA)	x								
German Microdata Lab (GML)				x		x			
Bundesanstalt für Arbeit (BA) im Institut für Arbeitsmarkt und Berufssforschung (IAB)			x						
ifo Institut – Leibniz-Institut für Wirtschaftsforschung	x								
Internationale Umfrageprogramme	x								
Institut zur Qualitätsentwicklung im Bildungswesen (IQB)	x	x							
Leibniz-Institut für Wirtschaftsforschung Halle (IWH)	x			x					
Forschungsinstitut zur Zukunft der Arbeit (IZA)	x		x						
Leibniz-Institut für Bildungsverläufe (LIfBi)	x	x							
Beziehungs- und Familienpanel pairfam	x								
Programme for the International Assessment of Adult Competencies (PIAAC)	x								
Robert Koch-Institut (RKI)	x								
RWI – Leibniz-Institut für Wirtschaftsforschung	x		x						
Survey of Health, Ageing and Retirement in Europe (SHARE)	x		x[1]			x			
Sozio-oekonomisches Panel (SOEP)	x		x[1]						
Statistische Ämter des Bundes und der Länder				x					
Stifterverband	x							x	
Wahlen	x								
Zentrum für Europäische Wirtschaftsforschung (ZEW)	x			x					
Leibniz-Zentrum für Psychologische Information und Dokumentation (ZPID)		x							

Hinweis: Stand September 2016. BDSG = Bundesdatenschutzgesetz, LDSG = Landesdatenschutzgesetz, SGB = Sozialgesetzbuch, BstatG = Bundesstatistikgesetz, KWG = Kreditwesengesetz, EU VO = EU Verordnung, UrhG = Urheberrechtsgesetz, UWG = Gesetz gegen unlauteren Wettbewerb, Sonst. = Sonstige, [1] = für verlinkte Sozialdaten.

Impressum

Herausgeber:
Rat für Sozial- und Wirtschaftsdaten (RatSWD)
Chausseestraße 111
10115 Berlin
office@ratswd.de
www.ratswd.de

Dieser Text wurde von folgenden Personen verfasst:
Tobias Gebel, *Universität Bielefeld*
Heike Habla, *Statistisches Bundesamt*
Dr. Cornelia Lange, *Robert Koch-Institut*
Alexia Meyermann, *Deutsches Institut für Internationale Pädagogische Forschung*
Prof. Regina T. Riphahn, Ph.D., *Friedrich-Alexander-Universität Erlangen-Nürnberg*
Daniel Schmidutz, *Max Planck Institute for Social Law and Social Policy*

Redaktion:
Dr. Jörg Holthöfer, Claudia Oellers, Thomas Runge

Gestaltung/Satz:
Markus Weiß | www.typogo.de

Berlin, Januar 2017

RatSWD Output:
Die RatSWD Output Series dokumentiert die Arbeit des RatSWD in seiner 5. Berufungsperiode (2014–2017). In ihr werden seine Stellungnahmen und Empfehlungen veröffentlicht und auf diesem Weg einer breiten Leserschaft zugänglich gemacht.

Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01UW1402 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt, sofern nicht anders ausgewiesen, beim RatSWD.

www.ratswd.de