SSOAR

Open Access Repository
www.ssoar.info

Handreichung Datenschutz

Veröffentlichungsversion / Published Version
Sonstiges / other

Empfohlene Zitierung / Suggested Citation:
Rat für Sozial- und Wirtschaftsdaten (RatSWD). (2020). *Handreichung Datenschutz.* (2. vollst. überarb. Auflage) (Output Series, 8 (6)). Berlin. https://doi.org/10.17620/02671.50

Nutzungsbedingungen:
Dieser Text wird unter einer Deposit-Lizenz (Keine Weiterverbreitung - keine Bearbeitung) zur Verfügung gestellt. Gewährt wird ein nicht exklusives, nicht übertragbares, persönliches und beschränktes Recht auf Nutzung dieses Dokuments. Dieses Dokument ist ausschließlich für den persönlichen, nicht-kommerziellen Gebrauch bestimmt. Auf sämtlichen Kopien dieses Dokuments müssen alle Urheberrechtshinweise und sonstigen Hinweise auf gesetzlichen Schutz beibehalten werden. Sie dürfen dieses Dokument nicht in irgendeiner Weise abändern, noch dürfen Sie dieses Dokument für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen.
Mit der Verwendung dieses Dokuments erkennen Sie die Nutzungsbedingungen an.

Terms of use:
This document is made available under Deposit Licence (No Redistribution - no modifications). We grant a non-exclusive, non-transferable, individual and limited right to using this document. This document is solely intended for your personal, non-commercial use. All of the copies of this documents must retain all copyright information and other information regarding legal protection. You are not allowed to alter this document in any way, to copy it for public or commercial purposes, to exhibit the document in public, to perform, distribute or otherwise use the document in public.
By using this particular document, you accept the above-stated conditions of use.

gesis Leibniz-Institut für Sozialwissenschaften

Mitglied der Leibniz-Gemeinschaft

Diese Version ist zitierbar unter / This version is citable under:
https://nbn-resolving.org/urn:nbn:de:0168-ssoar-68683-5

8 | Output
6. Berufungsperiode

RatSWD.
Rat für Sozial- und WirtschaftsDaten

Handreichung Datenschutz

2. vollständig überarbeitete Auflage

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Rat für Sozial- und Wirtschaftsdaten (RatSWD)

Handreichung Datenschutz

2. vollständig überarbeitete Auflage

überarbeitet von
Prof. Dr. Matthias Bäcker und Dr. Sebastian Golla
in Zusammenarbeit mit dem RatSWD

Abkürzungsverzeichnis

BDSG . . . . . Bundesdatenschutzgesetz
BStatG . . . . . Bundesstatistikgesetz
BVerfG . . . . . Bundesverfassungsgericht
DFG . . . . . Deutsche Forschungsgemeinschaft
DSGVO . . . . . EU-Datenschutz-Grundverordnung
DSK . . . . . Konferenz der unabhängigen Datenschutz-Aufsichtsbehörden des Bundes und der Länder
EuGH . . . . . Europäischer Gerichtshof
GG . . . . . Grundgesetz
i. V. m. . . . . in Verbindung mit
LDA . . . . . Landesbeauftragte für Datenschutz und Akteneinsicht
LDSG . . . . . Landesdatenschutzgesetz
LfDI . . . . . Landesbeauftragte/r für Datenschutz und Informationsfreiheit
lit. . . . . littera (Buchstabe)
RatSWD . . . . . Rat für Sozial- und Wirtschaftsdaten
SGB . . . . . Sozialgesetzbuch
UAbs. . . . . Unterabsatz
ULD . . . . . Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhaltsverzeichnis

Vorwort . . . 6

1 Einleitung . . . 7

2 Grundsätze der DSGVO . . . 8
2.1 Anwendungsbereich . . . 9
2.2 Verbotsprinzip und Rechtmäßigkeit der Verarbeitung . . . 10
2.3 Transparenz . . . 11
2.4 Zweckbestimmtheit und Zweckbindung . . . 11
2.5 Datenminimierung . . . 12
2.6 Speicherbegrenzung . . . 13
2.7 Integrität und Vertraulichkeit . . . 13
2.8 Technische und organisatorische Umsetzung der Grundsätze . . . 13

3 Anwendbare Regelungen neben der DSGVO . . . 14
3.1 Unions- und verfassungsrechtlicher Rahmen . . . 14
3.2 Bundesdatenschutzgesetz (BDSG) und Landesdatenschutzgesetze (LDSG) . . . 15
3.3 Bundes- und landesrechtliche Spezialregelungen . . . 15

4 Grundbegriffe des Datenschutzes für die Forschung . . . 17
4.1 Besondere Kategorien personenbezogener Daten . . . 17
4.2 Anonymisierung . . . 18
4.3 Pseudonymisierung . . . 19
4.4 Verantwortlichkeit . . . 20
4.5 Einwilligung . . . 21

5 Pflichten des Datenverarbeitenden . . . 23
5.1 Garantien für die Rechte und Freiheiten der Betroffenen . . . 23
5.2 Datensicherheit / Technische und organisatorische Maßnahmen . . . 23
5.3 Wahrung von Betroffenenrechten . . . 24
5.4 Führen eines Verfahrensverzeichnisses . . . 25
5.5 Bestellung eines Datenschutzbeauftragten . . . 26
5.6 Durchführung einer Datenschutz-Folgenabschätzung . . . 26

6 Datenakquise (bei der Feldarbeit) . . . 27
6.1 Auf Grundlage einer Einwilligung . . . 27
6.2 Auf gesetzlicher Grundlage . . . 28

7 Datenaufbereitung und Datenanalyse (nach der Feldarbeit) . . . 29

8 (Daten-)Publikation . . . 30

9 Aufbewahrung und sekundäre Nutzung von Forschungsdaten . . . 31
9.1 Aufbewahrung und Archivierung . . . 31
9.2 Sekundäre Nutzung . . . 32

10 Checklisten und Best Practices . . . 33
10.1 Grundlegende Fragen bei der Datenverarbeitung . . . 33
10.2 Weitere Überlegungen . . . 33
10.3 Best Practices . . . 34

11 Literaturverzeichnis . . . 36

Anhang . . . 38

Mitwirkende . . . 40

Vorwort

Der Rat für Sozial- und Wirtschaftsdaten (RatSWD) ist ein unabhängiges Gremium, das aus empirisch arbeitenden Wissenschaftlerinnen und Wissenschaftlern sowie Vertreterinnen und Vertretern von Datenproduzenten besteht. 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 zahlreichen, aktuell 38 Forschungsdatenzentren.

Im Rahmen dieses Mandates hat der RatSWD während seiner fünften Berufungsperiode (2014–2017) die erste Fassung der Handreichung zum Thema Datenschutz erstellt. Anfang 2020 wurde die Handreichung aufgrund der neuen Vorgaben für das Datenschutzrecht aus der EU-Datenschutz-Grundverordnung (DSGVO) grundlegend überarbeitet. Im Zentrum des Interesses der Handreichung steht der Umgang mit personenbezogenen Daten im Rahmen sozial-, verhaltens- und wirtschaftswissenschaftlicher Forschung.

1 Einleitung

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 näher zu bringen. Die Handreichung erläutert die datenschutzrechtlichen Grundsätze nach der DSGVO, die wichtigsten anwendbaren rechtlichen Regelungen neben der DSGVO, die Grundbegriffe des Datenschutzes in der Forschung und die Pflichten des Datenverarbeitenden. Spezifischer widmet sich die Handreichung datenschutzrechtlichen Aspekten bei der Akquise, Aufbereitung, Publikation und Aufbewahrung von Daten.

Das Interesse und der Bedarf der Sozial-, Verhaltens- und Wirtschaftswissenschaften an möglichst umfassenden und genauen Daten, der Nachvollziehbarkeit von Ergebnissen und der Nutzung von Daten für die Untersuchung unterschiedlichster Fragestellungen stehen oftmals in einem Spannungsverhältnis zu datenschutzrechtlichen Prinzipien wie der Speicherbegrenzung, der Datensparsamkeit und der Zweckbestimmung. Die Bereitschaft, Daten für Forschungsvorhaben verfügbar zu machen, steht in einem engen Zusammenhang mit dem verantwortungsvollen Umgang mit diesen Daten und dem damit verbundenen Vertrauen in die Integrität der Wissenschaft. Die Einhaltung der Datenschutzbestimmungen ist damit existenziell für die empirisch arbeitende Forschung.

Die Handreichung soll die Grundzüge des Rechtsgebiets vorstellen und auf die Herausforderungen aufmerksam machen. Die Forschung in den Sozial-, Verhaltens- und Wirtschaftswissenschaften ist so facettenreich, dass sich die möglichen datenschutzrechtlichen Fragestellungen nicht knapp und pauschal abhandeln lassen. Eine weitere Befassung mit dem Einzelfall wird meist unerlässlich sein. Die Konzeption von Forschungsprojekten, bei denen in großem Stil personenbezogene Daten verarbeitet werden, bedarf regelmäßig datenschutzrechtlicher Begleitung. Hinweise auf weiterführende Literatur und andere Quellen finden sich im Text. Zahlreiche Informationen zu einzelnen Datenschutzthemen finden sich – etwa in Form von Kurzpapieren – unter anderem auf den Internetauftritten der Datenschutzaufsichtsbehörden.[1] Die von diesen Stellen bereitgestellten Informationen sind auch deswegen besonders relevant, weil die Durchsetzung des Datenschutzrechts im Wesentlichen in ihren Händen liegt. Für die Auslegung der DSGVO sind die nicht unmittelbar verbindlichen, aber viel beachteten Leitlinien des Europäischen Datenschutzausschusses von Interesse.[2] Im Januar 2020 hat zudem der Europäische Datenschutzbeauftragte eine vorläufige Stellungnahme zum Datenschutz und zur wissenschaftlichen Forschung abgegeben.[3]

Obwohl zur Auslegung des Datenschutzrechts neben den Handreichungen der Behörden bereits zahlreiche Literaturquellen zur Verfügung stehen, sind viele praktisch wichtige Fragen ungeklärt oder zumindest nicht im Detail ausgeleuchtet. Dies wird auch die (derzeit noch spärliche) Rechtsprechung nicht in absehbarer Zeit leisten können, da sich die Rechtmäßigkeit von Datenverarbeitungen gerade im Forschungsbereich oftmals anhand von Interessenabwägungen oder anderen Betrachtungen im Einzelfall entscheidet, die ohne konkreten praktischen Bezug nicht vollständig zu antizipieren sind.

Gerade in der aktuellen Phase besteht die Möglichkeit für die Wissenschaft, die Entwicklung einer guten Datenschutzpraxis im Forschungsbereich mitzuprägen. Konkret bietet sich das etwa bei der Entwicklung ethischer Standards für die Erteilung von Einwilligungen (vgl. dazu 4.5) sowie von Kriterien für die Interessenabwägung im Rahmen von Art. 6 Abs. 1 lit. f DSGVO (vgl. dazu 2.2) und § 27 Abs. 1 Satz 1 BDSG (vgl. dazu 4.1) an.

1 Eine Übersicht der Kontaktdaten und Internetauftritte findet sich unter https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html.
2 Abrufbar unter https://edpb.europa.eu/edpb_de.
3 Abrufbar unter https://europa.eu/!WR73NV.

2 Grundsätze der DSGVO

Mit Geltung der EU-Datenschutz-Grundverordnung (DSGVO) ab dem 25. Mai 2018 hat im Datenschutzrecht eine neue Zeitrechnung begonnen. Zwar führt die DSGVO viele bekannte Prinzipien des Datenschutzrechts fort (Albrecht und Jotzo 2017: Teil 2 Rn 1). Allerdings enthält sie teilweise auch neue Pflichten für Datenverarbeitende und insbesondere hohe Strafandrohungen. Sie hat damit dem Datenschutzrecht zu einer bisher ungekannten Aufmerksamkeit verholfen, die eine Umsetzung der datenschutzrechtlichen Vorgaben als dringlich erscheinen lässt.

Neu ist mit der DSGVO, dass sich die Regeln über die Verarbeitung personenbezogener Daten in erster Linie direkt nach dem Recht der Europäischen Union richten. Regelungen aus dem nationalen Recht treten lediglich ergänzend hinzu (vgl. dazu unter 3). Dieser Abschnitt stellt die wichtigsten Prinzipien der Datenverarbeitung nach der DSGVO vor.

Die DSGVO enthält zahlreiche Privilegierungen von Datenverarbeitungen zu wissenschaftlichen Forschungszwecken. Hierfür sieht sie unter anderem Ausnahmen von den Grundsätzen der Zweckbestimmtheit und Zweckbindung (Art. 5 Abs. 1 lit. b Halbsatz 2 DSGVO, vgl. dazu näher 2.4) und der Speicherbegrenzung (Art. 5 Abs. 1 lit. e Halbsatz 2 DSGVO, vgl. dazu näher 2.6), Möglichkeiten zur Beschränkung bestimmter Betroffenenrechte (Art. 89 Abs. 2 DSGVO, Art. 14 Abs. 5 lit. b DSGVO, Art. 17 Abs. 3 lit. d DSGVO, Art. 21 Abs. 6 DSGVO, vgl. dazu näher 5.3) sowie die Möglichkeit zur Schaffung eines Grundes für die Verarbeitung besonderer Kategorien personenbezogener Daten zu Forschungszwecken (Art. 9 Abs. 2 lit. j DSGVO, vgl. dazu näher 4.1) vor. Spiegelbildlich zu diesen Privilegien enthält die DSGVO für die Verarbeitung von Daten zu wissenschaftlichen Forschungszwecken die Pflicht, „geeignete Garantien für die Rechte und Freiheiten der betroffenen Person“ vorzusehen (Art. 89 Abs. 1 Satz 1 DSGVO, vgl. dazu näher 5.1).

2.1 Anwendungsbereich

> *„Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“*
>
> *Art. 2 Abs. 1 DSGVO*

Die DSGVO findet Anwendung, wenn

- personenbezogene Daten vorliegen,
- die verarbeitet werden
- und dies entweder automatisiert oder in einem Dateisystem geschieht.

Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“. Als identifizierbar gilt „eine natürliche Person [...], die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“. Es muss also kein Name angegeben sein, damit eine Information Personenbezug hat. Es reicht, wenn eine Person beispielsweise über eine Kennziffer mit Zusatzwissen identifiziert werden kann. Es ist auch nicht notwendig, dass eine Information eine bestimmte inhaltliche Relevanz hat.

Der Personenbezug ist weit und kontextbezogen zu verstehen. Eine Information ist auch dann personenbezogen, wenn die Zuordnung zu einer Person einen gewissen Aufwand erfordert. Der Europäische Gerichtshof hat in seiner Rechtsprechung zuletzt u. a. dynamische IP-Adressen aus Sicht des Websitebetreibers (EuGH, Urteil vom 19.10.2016 – C-582/14) sowie Prüfungsantworten und Korrekturen (EuGH, Urteil vom 20.12.2017 – C-434/16) als personenbezogene Daten eingeordnet.

Ein Personenbezug ist auch anzunehmen, wenn Daten **pseudonymisiert** werden, sofern die Zuordnung zu einer Person wiederhergestellt werden kann (vgl. dazu näher 4.4). Nur eine **Anonymisierung** schließt den Personenbezug aus (vgl. dazu näher 4.3).

Die **Verarbeitung** bezeichnet nach Art. 4 Nr. 2 DSGVO „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“. Kurz gefasst beschreibt der Begriff der Verarbeitung jede Form des Umgangs mit personenbezogenen Daten. Auch das Löschen oder Veröffentlichen von Daten zählen hierzu.

Dass die Verarbeitung **automatisiert oder in einem Dateisystem** geschehen muss, schließt einzelne Datenverarbeitungsvorgänge vom Anwendungsbereich der DSGVO aus. Dies gilt etwa für das Anfertigen ungeordneter Notizen mit Personenbezug oder den Austausch von personenbezogenen Daten in mündlicher Form. Für öffentliche Forschungseinrichtungen ist diese Einschränkung des Anwendungsbereiches der DSGVO allerdings praktisch nicht relevant. Denn das Bundesdatenschutzgesetz und auch die Landesdatenschutzgesetze erklären die DSGVO hinsichtlich öffentlicher Stellen – zu denen auch staatliche Hochschulen und außeruniversitäre wissenschaftliche Forschungsinstitute zählen – auch für nicht-automatisierte Verarbeitungen sowie Verarbeitungen außerhalb von Dateisystemen für entsprechend anwendbar.

2.2 Verbotsprinzip und Rechtmäßigkeit der Verarbeitung

> *„Personenbezogene Daten müssen auf rechtmäßige Weise [...] verarbeitet werden.“*
>
> *Art. 5 Abs. 1 lit. a DSGVO*

Nach der DSGVO bedarf die Verarbeitung personenbezogener Daten stets einer Rechtfertigung, sie ist also **im Ausgangspunkt verboten**. Die DSGVO regelt in Art. 6 Abs. 1 die Fälle, in denen die Verarbeitung ausnahmsweise erlaubt ist. Dieser Katalog ist abschließend. Teilweise konkretisieren ihn jedoch weitere rechtliche Vorschriften, etwa in den Datenschutzgesetzen des Bundes und der Länder.

Praktisch zu beachten ist, dass es eines Grundes für **jede einzelne Datenverarbeitungshandlung** bedarf. Werden also etwa Daten erst erhoben, dann gespeichert, dann ausgewertet und anschließend veröffentlicht, so muss jeder dieser Schritte auf seine Zulässigkeit geprüft werden.

Als Rechtsgrundlagen der Datenverarbeitung kommen einerseits eine **Einwilligung** des Betroffenen (Art. 6 Abs. 1 lit. a DSGVO, vgl. dazu näher 4.6) und andererseits eine **gesetzliche Erlaubnis** in Betracht. Als gesetzliche Erlaubnisse sind für Forschende vor allem die Wahrnehmung von Aufgaben im öffentlichen Interesse (Art. 6 Abs. 1 lit. e DSGVO) und die Befugnis zur Datenverarbeitung nach einer allgemeinen Interessenabwägung (Art. 6 Abs. 1 lit. f DSGVO) relevant. Eine spezielle Erlaubnis zur Datenverarbeitung, die sich nur auf Forschungszwecke bezieht, enthält die DSGVO nicht. Art. 89 DSGVO enthält keine spezielle Erlaubnis für die Verarbeitung zu Forschungszwecken, sondern erlaubt den Mitgliedstaaten spezielle Sonderregelungen (bzgl. Betroffenenrechten, vgl. dazu unten 5.3) und gibt ihnen besondere Schutzmaßnahmen bzw. Garantien für die Verarbeitung zu Forschungszwecken auf. Das nationale Recht enthält besondere Forschungsklauseln in § 27 Abs. 1 BDSG und entsprechenden Vorschriften der Landesdatenschutzgesetze. Diese Erlaubnisse beziehen sich aber nicht auf die Verarbeitung personenbezogener Daten im Allgemeinen (nach Art. 6 DSGVO), sondern speziell auf die Verarbeitung besonderer Kategorien personenbezogener Daten (nach Art. 9 DSGVO, vgl. dazu näher 4.1).

Welche dieser Erlaubnisse in Frage kommt, hängt dabei davon ab, wie eine Forschungseinrichtung organisiert ist. **Öffentliche Forschungseinrichtungen** können sich grundsätzlich nicht auf die Befugnis zur Datenverarbeitung nach einer allgemeinen Interessenabwägung berufen. Sie müssen sich auf die Erfüllung ihrer Aufgaben stützen, d. h. die Wahrnehmung von Aufgaben im öffentlichen Interesse. Rechtsgrundlage für die Verarbeitung personenbezogener Daten zu Forschungszwecken ist dann Art. 6 Abs. 1 lit. e DSGVO in Verbindung mit einer nationalen Regelung, die die Forschungsaufgabe regelt. So sind etwa öffentlichen Hochschulen (Universitäten und Fachhochschulen) und außeruniversitären Forschungseinrichtungen durch die Hochschulgesetze der Länder ausdrücklich Forschungsaufgaben zugewiesen. Die Erlaubnisse der Hochschulen und der sonstigen öffentlichen Forschungseinrichtungen zur Datenverarbeitung zu Forschungszwecken sind damit in erster Linie durch die ihnen zugewiesenen Forschungsaufgaben begrenzt. Da die Datenverarbeitung zur Erfüllung der Forschungsaufgaben erforderlich sein muss, ist zweitens eine spezifische Interessenabwägung vorzunehmen. Diese kann sich nach den sogleich genannten Maßstäben richten.

Private Forschungseinrichtungen[4] können sich hingegen in der Regel nicht auf die Wahrnehmung von Aufgaben im öffentlichen Interesse berufen. Rechtsgrundlage für ihre Datenverarbeitung zu Forschungszwecken ist regelmäßig Art. 6 Abs. 1 lit. f DSGVO. Diese Vorschrift ermöglicht die Verarbeitung personenbezogener Daten, wenn sie zur Wahrung der berechtigten Interessen der

4 Bei der Unterscheidung zwischen privaten und öffentlichen Forschungseinrichtungen kommt es nicht auf die Organisationsform, sondern auf die Aufgabenzuweisung der jeweiligen Einrichtung an. So ist beispielsweise auch eine (g)GmbH, die von einem öffentlichen Träger beherrscht wird und der eine Forschungsaufgabe zugewiesen ist, als öffentliche Forschungseinrichtung einzuordnen. Wenn außerdem eine öffentliche Forschungseinrichtung Drittmittel von einer privaten Stelle (z. B. einem Unternehmen) einwirbt, wird das damit finanzierte Forschungsprojekt im Rahmen der öffentlichen Aufgabe durchgeführt. Anders liegt es etwa, wenn einzelne Forschende im Rahmen einer Nebentätigkeit ein Forschungsprojekt für eine private Stelle durchführen.

Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Die wissenschaftliche Forschung ist ein berechtigtes Interesse in diesem Sinne, das gegen die Interessen der Betroffenen **abzuwägen** ist. Auf der Seite der Betroffenen ist unter anderem zu berücksichtigen, wie sensibel die Daten sind (vgl. dazu auch 4.1), ob sie aus allgemein zugänglichen oder anderen Quellen stammen und ob der Betroffene mit einer (weiteren) Verarbeitung der Daten rechnen konnte. Es ist auch die Beziehung zwischen dem forschenden Datenverarbeitenden und dem Betroffenen zu berücksichtigen. Bei den Forschungsinteressen kommt es darauf an, welche Bedeutung die Verarbeitung spezifischer personenbezogener Daten für die Ausführung eines Forschungsvorhabens hat.

2.3 Transparenz

> *„Personenbezogene Daten müssen [...] in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.“*
>
> *Art. 5 Abs. 1 lit. a DSGVO*

Es ist ein zentrales Anliegen des Datenschutzrechts, dass der Umgang mit personenbezogenen Daten für den Betroffenen angesichts der Komplexität moderner Datenverarbeitungen **überschaubar** bleibt. Der Grundsatz der Transparenz findet dabei Ausprägung in verschiedenen Regelungen der DSGVO. So dient das Erfordernis, dass eine Einwilligung die Zwecke der Datenverarbeitung bestimmen muss (vgl. näher 4.5) ebenso der Nachvollziehbarkeit wie die Pflichten zur proaktiven Information des Betroffenen (vgl. näher 5.2). Auch das Auskunftsrecht (Art. 15 DSGVO) dient der Transparenz.

2.4 Zweckbestimmtheit und Zweckbindung

> *„Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.“*
>
> *Art. 5 Abs. 1 lit. b DSGVO*

Das Prinzip der Zweckbestimmtheit und Zweckbindung dient der **Überschaubarkeit und Kontrollierbarkeit** des Umgangs mit personenbezogenen Daten. Es erfordert zunächst, dass die Zwecke einer Datenverarbeitung schon bei der ersten Erhebung möglichst genau bestimmt werden, etwa in einer Einwilligungserklärung oder einem Forschungskonzept. Des Weiteren sind die weiteren Verarbeitungen grundsätzlich an den bestimmten Zweck gebunden. Eine Zweckänderung ist zwar möglich, bedarf aber einer Erlaubnis.

Speziell **für den Forschungsbereich lockert** die DSGVO das Prinzip der Zweckbestimmtheit und Zweckbindung allerdings. Damit reagiert das Recht auf den Umstand, dass Forschungsziele und -fragen häufig nicht abschließend im Vorfeld festgelegt werden können. Art. 5 Abs. 1 lit. b Halbsatz 2 DSGVO erklärt eine Weiterverarbeitung von Daten, die ursprünglich für andere Zwecke erhoben wurden, für wissenschaftliche oder historische Forschungszwecke nicht als unvereinbar mit den ursprünglichen Zwecken. Die Regelung wirkt als Fiktion der Vereinbarkeit der Weiterverarbeitung: Auch wenn die Forschungszwecke mit den ursprünglich verfolgten Zwecken nach den allgemeinen Beurteilungskriterien möglicherweise nicht mit dem ursprünglichen Verarbeitungszweck vereinbar wären, gibt die DSGVO eine solche Vereinbarkeit rechtlich vor. Der Datenverarbeitende kann sich daher bei der Weiterverarbeitung auf die gleiche Rechtsgrundlage stützen wie bei der ursprünglichen Verarbeitung.

Beispiel 1: Für ein Forschungsprojekt zur Korruptionsanfälligkeit bestimmter Wirtschaftssektoren sollen Akten von Gewerbeaufsichtsbehörden ausgewertet werden. Die darin liegende Zweckänderung der in den Akten enthaltenen personenbezogenen Daten, die ursprünglich der behördlichen Aufgabenerfüllung dienten, ist prinzipiell zulässig, obwohl die Zwecke der Forschung und der hoheitlichen Eingriffsverwaltung sich prima facie deutlich unterscheiden. Die Datenverarbeitung setzt allerdings – wie immer – zudem voraus, dass es eine Verarbeitungserlaubnis aus Art. 6 und ggfs. aus Art. 9 DSGVO gibt.

Beispiel 2: Im Rahmen eines langfristigen Forschungsprojekts zum Wandel weltanschaulicher Überzeugungen werden Daten erhoben, von denen sich später herausstellt, dass sie für eine kriminologische Untersuchung über die Straffälligkeit eines Subsets der Befragten fruchtbar sein könnten. Die kriminologische Untersuchung verfolgt einen neuen Verarbeitungszweck, da es sich um ein neues Forschungsprojekt mit einem neuen Erkenntnisziel handelt. Die Zweckänderung ist allerdings wiederum privilegiert. Wiederum bedarf die Datenverarbeitung allerdings eines Erlaubnistatbestands, der hinsichtlich des neuen Forschungszwecks eigenständig zu prüfen ist.

2.5 Datenminimierung

> *„Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.“*
>
> *Art. 5 Abs. 1 lit. c DSGVO*

Das Prinzip der Datenminimierung erfordert, dass der Umgang mit personenbezogenen Daten auf das **geringste Maß** beschränkt bleibt, das zur Erfüllung des verfolgten Zweckes erforderlich ist. Dieses Prinzip findet sich unter anderem in der Befugnis wieder, Daten im Rahmen des für die Erfüllung von öffentlichen Aufgaben oder zur Wahrung eines berechtigten Interesses Erforderlichen zu verarbeiten (Art. 6 Abs. 1 lit. e und f DSGVO).

Beispiel: In einer Studie, die Unterschiede bei den Konsumvorlieben von gleichgeschlechtlichen Paaren untersucht, dürfen keine Informationen über religiöse Anschauungen erhoben werden, wenn diese keine Rolle für den festgelegten Forschungszweck spielen.

Das Prinzip der Datenminimierung ist allerdings nicht derart eng auszulegen, dass sich das für die Zwecke der Verarbeitung notwendige Maß zwingend nach einer spezifischen Forschungsfrage bestimmt. Maßgeblich hierfür kann das übergeordnete Forschungsvorhaben sein, das den Zweck breiter festlegt. Hierbei ist andererseits das datenschutzrechtliche Gebot zu beachten, den Verarbeitungszweck so präzise wie möglich zu bestimmen. Es ist nicht möglich, sich den datenschutzrechtlichen Bindungen durch eine beliebig weite Zweckbestimmung (Extrembeispiel: „Datenverarbeitung für die sozialwissenschaftliche Forschung“) zu entziehen.

Das Prinzip der Datenminimierung kann in Konflikt mit der Forschung mit großen Datenmengen (**Big Data**) geraten. Gerade hier lässt sich unter Umständen aber auch argumentieren, dass die massenhafte Auswertung von personenbezogenen Daten notwendig ist, um ein Forschungsvorhaben durchzuführen. Insbesondere in solchen Fällen ist allerdings darauf zu achten, dass der Zweck des Forschungsvorhabens möglichst präzise beschrieben wird.

Beispiel: Auch die massenhafte Auswertung von personenbezogenen Daten aus Archiven oder sozialen Netzwerken kann als auf das notwendige Maß beschränkt gelten, wenn wissenschaftlich plausibel gemacht wird, dass sich hierdurch Korrelationen erkennen und Erkenntnisse gewinnen lassen, die mit kleineren Datenmengen nicht möglich wären. Unzulässig wäre hingegen etwa eine Analyse von Korrelationen “ins Blaue hinein”, die nicht von einem vorab möglichst präzise festgelegten Erkenntnisziel ausginge.

2.6 Speicherbegrenzung

> *„Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.“*
>
> *Art. 5 Abs. 1 lit. e DSGVO*

Das Prinzip der Speicherbegrenzung ist mit dem Prinzip der Datenminimierung verwandt. Es erfordert, dass personenbezogene Daten gelöscht werden, wenn sie für die mit ihrer Verarbeitung verfolgten Zwecke nicht mehr benötigt werden. Damit stellt es eine **zeitliche Grenze** für die Verarbeitung personenbezogener Daten auf.

Für die Datenverarbeitung zu Forschungszwecken gilt allerdings nach Art. 5 Abs. 1 lit. e Halbsatz 2 DSGVO eine Ausnahme vom Grundsatz der Speicherbegrenzung. Diese Regelung ermöglicht eine längere Speicherung von personenbezogenen Daten, wenn zu dem ursprünglich verfolgten Zweck ihrer Verarbeitung ein Forschungszweck hinzutritt, der eine längere Speicherung erfordert, z. B. im Rahmen von Sekundäranalysen. Es ist hierbei jedoch das für die wissenschaftliche Forschung geltende Gebot zu beachten, personenbezogene Daten nach Möglichkeit zu anonymisieren oder zu pseudonymisieren (vgl. dazu unten 4.2 und 4.3).

2.7 Integrität und Vertraulichkeit

> *„Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.“*
>
> *Art. 5 Abs. 1 lit. f DSGVO*

Der Grundsatz der Integrität und Vertraulichkeit zielt vor allem auf die **technische Sicherheit** von Daten. Zu dieser enthalten Art. 32 DSGVO allgemeine und Art. 89 DSGVO weitere, auf die Forschung bezogene Vorgaben, auf die unten im Einzelnen näher eingegangen werden soll (vgl. 5.2).

2.8 Technische und organisatorische Umsetzung der Grundsätze

Nach Art. 25 Abs. 1 DSGVO hat der Verantwortliche „geeignete technische und organisatorische Maßnahmen“ zu treffen, „die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.“

Daraus folgt die Verpflichtung, schon bei der technischen und organisatorischen Gestaltung von Datenverarbeitungsprozessen die genannten Grundsätze des Datenschutzrechts zu beachten (**Privacy by Design**). Die DSGVO reagiert damit darauf, dass das Recht in Bezug auf einzelne Datenverarbeitungshandlungen nur eine begrenzte Wirkungsmacht hat, wenn durch die vorgelagerte technische und organisatorische Ausgestaltung Sachzwänge entstehen.

Hieraus lassen sich auch die technischen Grundsätze der Datenvermeidung und Datensparsamkeit ableiten: Schon bei der Gestaltung von Datenverarbeitungstechnologien und ihren Voreinstellungen ist darauf hinzuwirken, dass möglichst wenige personenbezogene Daten verarbeitet werden.

Beispiel: Bei der Programmierung einer Forschungs-App für ein Mobiltelefon dürfen die Möglichkeiten eines Zugriffs auf die Kamera und die Standorterkennung des Geräts gar nicht erst technisch vorgesehen werden, wenn diese Informationen nicht für den Forschungszweck benötigt werden.

3 Anwendbare Regelungen neben der DSGVO

Auch wenn die DSGVO das wichtigste Regelungswerk für den (Forschungs-)Datenschutz ist, ist sie hierfür nicht allein maßgeblich. Zusätzlich ist der verfassungsrechtliche Rahmen des Datenschutzes in der EU und Deutschland zu beachten (3.1).

Teilweise ergänzen außerdem nationale Regelungen die DSGVO bezüglich der Verarbeitung personenbezogener Daten zu Forschungszwecken (3.2 – 3.4). Dies ist allerdings nur möglich, soweit die vorrangige DSGVO ausdrücklich Spielräume für ergänzende Regelungen eröffnet.

3.1 Unions- und verfassungsrechtlicher Rahmen

> *„Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten."*
>
> *Art. 8 Abs. 1 Charta der Grundrechte der Europäischen Union*

Die **verfassungsrechtliche Basis für das Datenschutzrecht** findet sich auf europäischer Ebene in dem Recht auf den Schutz personenbezogener Daten aus Art. 8 Charta der Grundrechte der Europäischen Union. Nach Art. 8 Abs. 2 Satz 1 Charta der Grundrechte der Europäischen Union dürfen personenbezogene Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Im deutschen Verfassungsrecht ist für den Datenschutz das Recht auf informationelle Selbstbestimmung maßgeblich. Dieses ist nicht explizit im Grundgesetz verankert, ergibt sich aber aus Art. 2 Abs. 1 (Recht auf freie Entfaltung der Persönlichkeit) in Verbindung mit Art. 1 Abs. 1 (Schutz der Menschenwürde) Grundgesetz. Da seit Mai 2018 mit der DSGVO ein Rechtsakt der Europäischen Union das Datenschutzrecht direkt regelt, sind allerdings primär die Vorgaben der Charta der Grundrechte der Europäischen Union maßgeblich.

> *„Kunst und Forschung sind frei. Die akademische Freiheit wird geachtet."*
>
> *Art. 13 Charta der Grundrechte der Europäischen Union*

Auch die **wissenschaftliche Forschung** ist verfassungsrechtlich geschützt. Art. 3 Abs. 3 UAbs. 1 Satz 3 Vertrag über die Europäische Union nennt den wissenschaftlichen Fortschritt gleichrangig mit dem nachhaltigen wirtschaftlichen Wachstum und dem sozialen Fortschritt als Zielbestimmung der Europäischen Union. Nach Art. 179 Abs. 1 Vertrag über die Arbeitsweise der Europäischen Union soll dafür ein europäischer Raum der Forschung geschaffen werden. Die Verarbeitung personenbezogener Daten zu Forschungszwecken ist eine wesentliche Grundbedingung, um dieses Ziel zu erreichen. Daneben schützen Art. 11 (Freiheit der Meinungsäußerung und Informationsfreiheit) und Art. 13 Charta der Grundrechte der Europäischen Union (Freiheit der Wissenschaft) die individuelle Forschungsfreiheit. Die Freiheit der Wissenschaft schützt dabei jedwede Tätigkeit mit dem Ziel, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen, sowie die Publikation wissenschaftlicher Ergebnisse. Sowohl natürliche Personen, die eigenverantwortlich wissenschaftlich tätig sind, als auch juristische Personen, insbesondere Hochschulen und außeruniversitäre Forschungseinrichtungen, können sich auf die Forschungsfreiheit berufen. In Deutschland ist die Forschungsfreiheit nach Art. 5 Abs. 3 Satz 1 Grundgesetz gewährleistet.

3.2 Bundesdatenschutzgesetz (BDSG) und Landesdatenschutzgesetze (LDSG)

Die DSGVO enthält Öffnungsklauseln, die es den nationalen Gesetzgebern erlauben, hinsichtlich bestimmter Fragen – etwa bei Datenverarbeitungen zur Erfüllung gesetzlicher Pflichten und öffentlicher Aufgaben (Art. 6 Abs. 2 und 3 DSGVO), im Zusammenhang mit der Meinungs- und Informationsfreiheit (Art. 85 DSGVO), zur Beschränkung von Betroffenenrechten (Art. 23 DSGVO) und im Zusammenhang mit der wissenschaftlichen Forschung (vgl. etwa Art. 9 Abs. 2 lit. j DSGVO und Art. 89 Abs. 2 DSGVO) – eigene ergänzende oder einschränkende Regelungen zum Datenschutz zu treffen. Solche Regelungen finden sich zunächst in den Datenschutzgesetzen des Bundes und der Länder. Das BDSG gilt grundsätzlich für öffentliche Stellen des Bundes[5] und für nicht-öffentliche Stellen (§ 1 Abs. 1 BDSG). Die Landesdatenschutzgesetze gelten für öffentliche Stellen der Länder.

Das BDSG wie auch die Landesdatenschutzgesetze enthalten **Sonderregelungen für Datenverarbeitungen zu Forschungszwecken**. Da sich die Regelungen inhaltlich stark ähneln, sollen sie exemplarisch anhand von § 27 BDSG vorgestellt werden, zu dem Parallelvorschriften in den Landesdatenschutzgesetzen existieren. § 27 Abs. 1 BDSG erlaubt die Verarbeitung besonderer personenbezogener Daten (vgl. 4.1) bei erheblich überwiegenden Forschungsinteressen. § 27 Abs. 4 BDSG trifft eine zusätzliche strengere Regelung für die Veröffentlichung von Daten (vgl. 8). § 27 Abs. 2 BDSG sieht für die Datenverarbeitung zu Forschungszwecken Ausnahmen von bestimmten Betroffenenrechten der DSGVO (vgl. 5.3) vor. § 27 Abs. 3 BDSG enthält ein besonderes Gebot, zu Forschungszwecken verarbeitete Daten zu anonymisieren (vgl. 4.2).

3.3 Bundes- und landesrechtliche Spezialregelungen

Neben BDSG und Landesdatenschutzgesetzen gelten für die Datenverarbeitung zu Forschungszwecken eine Reihe von bundes- und landesrechtlichen Spezialvorschriften, die jeweils nur bestimmte Forschungsgegenstände oder Forschungsmethoden betreffen.

Im **Bundesrecht** finden sich spezielle Regelungen etwa im Arzneimittelgesetz, dem Gendiagnostikgesetz, dem Transplantationsgesetz und dem Stasi-Unterlagengesetz. Für die Forschung mit Melderegisterdaten sind die Vorschriften des Bundesmeldegesetzes zu beachten (vgl. hierzu von Lewinski 2017: 1 ff.).

Der Schutz von **Sozialdaten**[6] ist in §§ 67 ff. SGB X umfassend geregelt. Er folgt im Wesentlichen den gleichen Prinzipien wie der Schutz sonstiger personenbezogener Daten, unterliegt aber im Einzelnen strengeren Anforderungen (vgl. Kipker und Pollmann 2019: 718 ff.). §§ 67a ff. SGB X regeln spezielle Befugnisse für die Verarbeitung von Sozialdaten. Werden diese nicht direkt bei der betroffenen Person erhoben, hängt die Rechtmäßigkeit der Erhebung im Wesentlichen von einer Interessenabwägung ab (vgl. § 67a Abs. 2 SGB X).

5 Für öffentliche Stellen der Länder gilt es nur ausnahmsweise, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie Bundesrecht ausführen oder als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

6 Dies sind personenbezogene Daten, die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach dem SGB I verarbeitet werden.

Die **Übermittlung** von Sozialdaten zu Forschungszwecken gestattet § 75 Abs. 1 Satz 1 Nr. 1 SGB X, wenn sie für ein bestimmtes Forschungsvorhaben im Sozialleistungsbereich oder in der wissenschaftlichen Arbeitsmarkt- und Berufsforschung erforderlich sind. Auch hier sind die Interessen der betroffenen Person im Einzelfall zu betrachten. Satz 2 der Vorschrift verpflichtet die übermittelnde Stelle[7] allerdings grundsätzlich dazu, eine Einwilligung einzuholen, wenn dies zumutbar ist und nicht nur grundlegende Informationen wie Name und Anschrift übermittelt werden sollen. § 75 Abs. 4 SGB X macht die Übermittlung zusätzlich von einer behördlichen Genehmigung abhängig.

In § 67b Abs. 2 und Abs. 3 SGB X finden sich zudem **besondere Regelungen für die Einwilligung** in die Verarbeitung von Sozialdaten. Nach § 67b Abs. 3 Satz 1 kann die Einwilligung zur Verarbeitung personenbezogener Daten zu Forschungszwecken für ein bestimmtes Vorhaben oder für bestimmte Bereiche der wissenschaftlichen Forschung erteilt werden. Die Regelung erlaubt damit eine weite Festlegung der Verarbeitungszwecke (vgl. näher zum „broad consent“ 4.5).

Auch bereichsspezifische **Landesgesetze** enthalten zum Teil kleinteilige Regelungen zum Umgang mit personenbezogenen Daten zu Forschungszwecken. Hierzu zählen etwa die Schulgesetze, die Landeskrankenhausgesetze und die Landesarchivgesetze. Daten der Statistischen Ämter des Bundes und der Länder sind durch die Statistikgesetze besonders geschützt. Für Angaben, die zu statistischen Zwecken gemacht werden, gilt ein besonderes Statistikgeheimnis (nach § 16 BStatG und entsprechenden Vorschriften der Landesgesetze). Sie dürfen nach § 16 Abs. 6 BStatG zu Forschungszwecken nur in faktisch oder formal anonymisierter Form übermittelt oder zugänglich gemacht werden. Es gilt eine strenge Zweckbindung und eine Pflicht zur Löschung nach Durchführung des konkreten Forschungsvorhabens (§ 16 Abs. 8 BStatG).

7 Beispielsweise das Forschungsdatenzentrum der Bundesagentur für Arbeit im Institut für Arbeitsmarkt- und Berufsforschung (FDZ der BA im IAB) oder der Rentenversicherung (FDZ-RV).

4 Grundbegriffe des Datenschutzes für die Forschung

Dieser Abschnitt stellt zentrale Grundbegriffe des Datenschutzes vor, die für die Verarbeitung von personenbezogenen Daten zu Forschungszwecken von Bedeutung sind.

4.1 Besondere Kategorien personenbezogener Daten

> *„Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.“*
>
> *Art. 9 Abs. 1 DSGVO*

Die DSGVO sieht für einige Arten personenbezogener Daten einen **zusätzlichen Schutz** vor. Die in Art. 9 Abs. 1 DSGVO genannten Daten sind nach der Wertung des Verordnungsgebers besonders sensibel. Die Regelung ist auch für die sozialwissenschaftliche Forschung relevant; beispielsweise können Informationen über politische Einstellungen oder Religionszugehörigkeit oder Gesundheitsdaten aus der Krankenversicherung im Rahmen sozialwissenschaftlicher Milieustudien von Interesse sein.

Damit die Verarbeitung derartiger Daten zulässig ist, müssen neben den allgemeinen Voraussetzungen aus Art. 6 DSGVO **zusätzlich** die Voraussetzungen von Art. 9 Abs. 2 DSGVO erfüllt sein. Diese Vorschrift sieht mehrere Varianten vor, nach denen eine Verarbeitung gerechtfertigt werden kann. Eine Variante ist die Erteilung einer Einwilligung, die sich ausdrücklich auf die Verarbeitung besonderer personenbezogener Daten bezieht (Art. 9 Abs. 2 lit. a DSGVO, vgl. dazu 4.5).

Eine weitere Möglichkeit zur Rechtfertigung der Verarbeitung bestimmter **öffentlich verfügbarer Daten** ergibt sich aus Art. 9 Abs. 2 lit. e DSGVO. Dieser gestattet die Verarbeitung besonderer personenbezogener Daten, die der Betroffene offensichtlich selbst öffentlich gemacht hat. In diesen Fällen fehlt es an einer besonderen Schutzbedürftigkeit. Diese Norm gestattet beispielsweise die Auswertung von Beiträgen in offenen Bereichen sozialer Netzwerke zu Forschungszwecken, sofern es nur um Informationen über die Verfasser der Beiträge selbst geht (Golla/Hofmann/Bäcker 2018: 92). Zu beachten ist, dass diese Erlaubnis nicht anwendbar ist, wenn eine andere als die betroffene Person die Daten veröffentlicht hat.

Noch interessanter ist für Forschende allerdings die Regelung in Art. 9 Abs. 2 lit. j DSGVO. Diese ermöglicht es den Mitgliedstaaten, eigene Regelungen für die Verarbeitung besonderer Kategorien personenbezogener Daten zu **Forschungszwecken** zu schaffen. Von dieser Möglichkeit hat der deutsche Gesetzgeber in § 27 BDSG Gebrauch gemacht (vgl. 3.2). Ähnliche Regelungen finden sich in den Datenschutzgesetzen der Länder. Die folgenden Ausführungen zu § 27 BDSG lassen sich daher weitgehend auf die Regelungen in den Landesgesetzen übertragen.

Aus § 27 Abs. 1 Satz 1 BDSG ergeben sich drei Voraussetzungen dafür, dass eine Verarbeitung besonderer personenbezogener Daten zu Forschungszwecken erlaubt ist:

1. Es muss ein **Zweck wissenschaftlicher Forschung** vorliegen. Dafür ist ein konkretes Forschungsvorhaben notwendig, das dem Aufbau und Inhalt nach wissenschaftlichen Ansprüchen genügt.

2. Die Datenverarbeitung muss zur **Durchführung dieses Vorhabens erforderlich** sein. Dies bedeutet, dass das Vorhaben ohne die Verarbeitung der konkreten personenbezogenen Daten undurchführbar wäre. Dabei ist auch die Möglichkeit zu berücksichtigen, dass Daten pseudonymisiert und anonymisiert werden können. Ist ein Vorhaben ebenso mit pseudonymisierten Daten oder anonymisierten Daten durchführbar, ist die Verarbeitung personenbezogener Daten nicht erforderlich. Es ist eine **Interessenabwägung im Einzelfall** vorzunehmen, bei der das wissenschaftliche Interesse das Interesse des Betroffenen im Ergebnis erheblich überwiegen muss. Durch das Wörtchen „erheblich" stellt § 27 Abs. 1 Satz 1 BDSG strengere Anforderungen an die Datenverarbeitung als die allgemeine Interessenabwägung nach Art. 6 Abs. 1 lit. e oder f DSGVO. Um zuverlässig beurteilen zu können, wann ein Forschungsinteresse erheblich überwiegt, werden für einzelne Forschungsbereiche praktische Leitlinien zu entwickeln sein. Diese Leitlinien können (und sollten) Forschende selbst gemeinsam mit den Datenschutzbeauftragten ihrer Institution sowie ggfs. Vertretern von Aufsichtsbehörden entwerfen. Sie haben dadurch die Möglichkeit, eigene Standards datenschutzfreundlicher Forschung zu etablieren.

Die Interessenabwägung wird in der Regel der **Schwerpunkt der Prüfung** sein, ob eine Datenverarbeitung nach § 27 Abs. 1 Satz 1 BDSG rechtmäßig ist. Dabei sind die wissenschaftlichen Interessen und das Interesse des Betroffenen zu gewichten. Für das wissenschaftliche Interesse spielt es eine Rolle, welche Bedeutung speziell die Verarbeitung besonderer Kategorien personenbezogener Daten für die Durchführung eines Forschungsvorhabens hat. Die Bedeutung eines Vorhabens verallgemeinernd zu gewichten, fällt hingegen schwer und stünde im Konflikt mit der Forschungsfreiheit. Auf der Seite des Betroffenen stellt sich die Frage, mit welcher Intensität Art. 9 Abs. 1 DSGVO betroffen ist, zu welchem Grad die dort genannten Merkmale also aus den verarbeiteten Daten hervorgehen (so können Datensätze beispielsweise klare Aussagen oder aber nur Indikatoren zu den religiösen Überzeugungen einer Person enthalten).

Beispiel: Es kommt für ein Forschungsvorhaben entscheidend auf die Berücksichtigung von Informationen über politische Meinungen an. Diese werden aber für jeden Betroffenen nur in einem eng umrissenen Rahmen verarbeitet. Dies spricht für ein erheblich überwiegendes Forschungsinteresse.

Des Weiteren hat der für die Datenverarbeitung Verantwortliche nach § 27 Abs. 1 Satz 2 BDSG angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Diese überschneiden sich weitgehend mit den nach Art. 89 DSGVO vorgesehenen geeigneten Garantien (vgl. 5.1) und den nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (vgl. 5.2).

Weitere Informationen zu den Anforderungen beim Umgang mit besonderen Kategorien personenbezogener Daten bieten die Datenschutzbehörden (DSK 2018h).

4.2 Anonymisierung

Anonymisierung bedeutet die **Tilgung des Personenbezugs** von Daten. Sind Daten anonymisiert, ist die DSGVO auf ihre Verarbeitung nicht mehr anwendbar (vgl. 2.1). Anders als die alte Fassung des BDSG enthält die DSGVO keine Definition des Begriffs Anonymisieren.[8] Die DSGVO nimmt aber Bezug auf das Konzept der Anonymisierung. Erwägungsgrund 26 DSGVO legt nahe, dass es bei der Tilgung des Personenbezugs auf eine faktische Anonymisierung ankommt, die gegeben ist, wenn ein Personenbezug nur mit unverhältnismäßig hohem Aufwand wiederhergestellt werden kann.

Das Datenschutzrecht enthält besondere **Anonymisierungsgebote für die Forschung**. Art. 89 Abs. 1 Satz 4 DSGVO verlangt, die Weiterverarbeitung von Daten zu Forschungszwecken wenn möglich in

8 Nach § 3 Abs. 6 BDSG alte Fassung war 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."

einer Form durchzuführen, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist. Daraus ist ein Gebot abzuleiten, Daten bei ihrer Verarbeitung zu Forschungszwecken nach Möglichkeit zu pseudonymisieren oder zu anonymisieren (Golla 2019: 658 f.). Ein besonderes Gebot der Anonymisierung enthält auch § 27 Abs. 3 Satz 1 BDSG für besondere Kategorien personenbezogener Daten (vgl. 4.1), die zu Forschungszwecken verarbeitet werden.

Diese Gebote der Anonymisierung lassen sich als Ausdruck der Prinzipien der **Datenminimierung** (vgl. 2.5) und **Speicherbegrenzung** (vgl. 2.7) verstehen (Johannes und Richter 2017: 302). Die Erreichung von Forschungszwecken mit anonymisierten Daten dürfte sich gerade in der sozialwissenschaftlichen Forschung allerdings in vielen Fällen als schwierig erweisen (Arning/Forgó/Krügel 2006: 701). Oft wird es auch die Nachvollziehbarkeit von Forschungsergebnissen erfordern, dass Daten nicht anonymisiert werden, da dieser Vorgang unumkehrbar ist. So wird in vielen Fällen nur die Möglichkeit der Pseudonymisierung als mildere Alternative zur Anonymisierung in Betracht kommen.

Technisch kommen für die Anonymisierung Methoden zur Veränderung und Reduktion des Informationsgehalts der Daten selbst in Betracht, wie z. B. Löschung der Identifikationsmerkmale, Merkmalsaggregation oder Maskierungen. Eine wirksame Anonymisierung ist allerdings kein trivialer Vorgang, da stets überprüft werden muss, ob die Herstellung eines Personenbezuges bzw. die De-Anonymisierung durch Zusatzwissen oder neuartige technische Methoden möglich ist. Eine einmalige Anonymisierung kann daher nicht mit Sicherheit als dauerhaft wirksam angesehen werden. Die Wirksamkeit einer Anonymisierung muss nach dem aktuellen Stand der Technik in gewissen Zeitabständen überprüft werden.

Beispiel: Die Daten aus einer Befragung werden unter Codes gespeichert, die sich aus persönlichen Informationen über die Befragten ergeben. Die Codes haben vier Stellen und setzen sich aus dem ersten Buchstaben des Vornamens von Mutter, Vater, befragter Person und der letzten Ziffer des Geburtsjahrs zusammen (also etwas MAS8 für Monika, Anton, Sandra, geboren 1968). Aus diesen Informationen kann durch den Abgleich mit Datenbeständen unter Umständen wieder auf die befragte Person geschlossen werden, so dass keine sichere Anonymisierungsmethode vorliegt.

Gangbar wäre hingegen etwa folgender Weg: Den erhobenen Daten wird eine laufende Kennziffer oder eine Zufallszahl zugewiesen. Solange für den Forschungszweck ggfs. eine konkrete Zuordnung zum einzelnen Probanden erforderlich ist (etwa, weil später noch weitere Daten erhoben werden sollen), wird eine Zuordnungstabelle gespeichert; in diesem Zeitraum sind die Daten pseudonymisiert. Ist die Zuordnung nicht mehr erforderlich, wird die Zuordnungstabelle gelöscht. Hierdurch werden die Daten anonymisiert, wenn sich auch aus ihrem Inhalt keine Rückschlüsse auf die betroffene Person ziehen lassen. Sind solche Rückschlüsse hingegen möglich, sind die Daten nicht anonymisiert.

4.3 Pseudonymisierung

> *„‘Pseudonymisierung‘ [ist] die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.“*
>
> *Art. 4 Nr. 5 DSGVO*

Bei der Pseudonymisierung wird der Personenbezug von Daten anders als bei der Anonymisierung nicht vollständig beseitigt. Identifizierende Informationen werden durch andere Merkmale ersetzt und gesondert aufbewahrt. Das Datenschutzrecht bleibt auf pseudonymisierte Daten anwendbar.

Beispiel: In einem Datensatz werden die Namen der betroffenen Personen durch Kennziffern ersetzt. Die Personen sind in dem Datensatz nicht durch weitere Merkmale identifizierbar. Die Liste mit der Zuordnung der Kennziffern wird bei einem Treuhänder hinterlegt.

Sofern sich Forschungszwecke durch die Verarbeitung pseudonymisierter Daten erreichen lassen, ist die **Pseudonymisierung geboten**, wie sich aus Art. 89 Abs. 1 Satz 3 DSGVO ergibt. Ein ähnliches Gebot enthält § 27 Abs. 3 Satz 2 BDSG. Auch diese Vorgaben sind Ausdruck der Prinzipien der Datenminimierung (vgl. 2.5) und Speicherbegrenzung (vgl. 2.7). Eine Pseudonymisierung wird oftmals eher eine realistische Alternative zur personenbezogenen Datenverarbeitung darstellen als die Anonymisierung, da sie es den Forschenden ermöglicht, ihre Datenbestände nachvollziehbar zu halten.

4.4 Verantwortlichkeit

> *„Im Sinne dieser Verordnung bezeichnet der Ausdruck ‚Verantwortlicher' die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet."*
>
> *Art. 4 Nr. 7 DSGVO*

Die Festlegung des Verantwortlichen bestimmt, wer die Bestimmungen des Datenschutzrechts einhalten muss und gegenüber wem Betroffene ihre Rechte in der Praxis ausüben können. Wer in der Forschung Verantwortlicher für die Datenverarbeitung anzusehen ist, ist nicht einfach zu beantworten. Maßgeblich ist nach Art. 4 Nr. 7 DSGVO, wer über **Zweck und Mittel einer Datenverarbeitung entscheidet**.

Dafür kommt es auf den tatsächlichen Einfluss auf die Datenverarbeitung an. Kriterien für die Entscheidungsbefugnis sind Weisungsrechte, das Auftreten gegenüber den Betroffenen, die traditionelle Rolle und Fachkompetenz der verschiedenen Beteiligten sowie deren Handlungsspielräume im konkreten Fall. Der Verantwortliche kann sich zur Datenverarbeitung eigener Hilfspersonen (insbesondere Angestellter und Beamter) sowie externer Auftragsverarbeiter (sonstiger durch Dienst- oder Werkvertrag mit Datenverarbeitungen betrauter Stellen) bedienen. Diese können bei ihrer Tätigkeit durchaus erhebliche **Spielräume** haben.

Sofern die genannten Kriterien erfüllt sind, wird sich auch an größeren Forschungseinrichtungen (wie z. B. Universitäten) eine **zentrale Verantwortlichkeit** annehmen lassen. Auch wenn den einzelnen Forschenden eine relativ große Freiheit zukommt, treten sie nach außen für die Einrichtung auf und erfüllen einen ihr zugewiesenen Auftrag.

Gemäß Art. 26 DSGVO können auch mehrere Stellen für eine Datenverarbeitung **gemeinsam verantwortlich** sein. Eine gemeinsame Verantwortlichkeit kommt etwa in Betracht,

- wenn im Rahmen größerer Forschungsprojekte verschiedene Einrichtungen miteinander kooperieren,
- wenn Survey-Programme Datenerhebungen bei Umfrageinstituten in Auftrag geben und diese einen gewissen Handlungsspielraum bei der Planung und Durchführung der Umfrage genießen,
- wenn Forschende ihre Forschungsdaten in Repositorien ablegen und ggf. für Sekundäranalysen verfügbar machen.

4.5 Einwilligung

> *„Im Sinne dieser Verordnung bezeichnet der Ausdruck ‚Einwilligung' der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist."*
>
> *Art. 4 Nr. 11 DSGVO*

Die Einwilligung ist im Forschungskontext eine wichtige Rechtsgrundlage zur Verarbeitung personenbezogener Daten. Sie kann sowohl die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 2 lit. a DSGVO, vgl. dazu näher oben 4.1) als auch sonstiger personenbezogener Daten (Art. 6 Abs. 1 lit. a DSGVO) rechtfertigen. Oft werden Einwilligungen aus Gründen der Rechtssicherheit gesetzlichen Verarbeitungsgründen vorgezogen. Dabei sollte das Potential der gesetzlichen Erlaubnisse jedoch nicht unterschätzt werden (vgl. 6.3). Eine Einwilligung kann aber auch unter ethischen Gesichtspunkten empfehlenswert sein (nach dem Prinzip „informed consent").

Art. 4 Nr. 11 DSGVO erfordert, dass die Einwilligung **freiwillig** erteilt wird. Dafür darf kein (gefühlter) Zwang oder ein erhebliches Machtungleichgewicht zwischen Verarbeiter und Betroffenem vorliegen, das sich auf die Erteilung der Einwilligung auswirkt.

Eine wichtige Grundbedingung für die Freiwilligkeit der Einwilligung ist, dass diese **informiert** erteilt wird. In der Forschung ist hierfür eine allgemeinverständliche Beschreibung von Forschungskonzepten und -zielen wichtig. In manchen Fällen steht die vollständige Information des Betroffenen im Konflikt mit der Forschungsmethode – so etwa bei psychologischen Experimenten, die mit gezielten Manipulationen arbeiten. Auch dies schließt es jedoch nicht aus, zumindest das Ziel der Forschung anzugeben. Eine Manipulation innerhalb eines Experiments kann damit in einem gewissen Rahmen zulässig sein, wenn nicht die Betroffenen gerade durch die Manipulation erst grundsätzlich dazu gebracht werden, personenbezogene Daten preiszugeben. In anderen Fällen kann die Informiertheit ein unüberwindbares Hindernis darstellen, wenn etwa das Forschungsvorhaben den Betroffenen kulturell oder intellektuell nicht vermittelbar ist.

Beispiel: Ein Hochschullehrer fordert die Studierenden in seinem Kurs zur Teilnahme an einem Experiment zur Verhaltensforschung auf und bittet sie um ihre Einwilligung in die Datenverarbeitung. Über den genauen Umgang mit ihren Daten sowie das Ziel des Experiments möchte er sie im Nachgang informieren. In diesem Fall ist die Freiwilligkeit zweifelhaft, da zwischen Lehrendem und Studierenden ein Über-/Unterordnungsverhältnis besteht und letztere sich zur Teilnahme verpflichtet fühlen könnten. Jedenfalls fehlt es an der Informiertheit, die vor der Datenverarbeitung hergestellt werden muss.

Außerdem muss die Einwilligung grundsätzlich für einen **bestimmten Fall** erteilt werden. Dies stellt für den Forschungsbereich eine Herausforderung dar, da sich Forschungsziele und -fragen nicht immer im Vorfeld präzise festlegen lassen. Aus diesem Grund ist für den Bereich der Forschung wichtig, dass eine Einwilligung auch mit einer weiten Zweckfestlegung (**„broad consent"**) erteilt werden kann. Dadurch wird zwar nicht das Gebot der Zweckbestimmtheit und Zweckbindung (vgl. dazu oben 2.4) eingeschränkt, wohl aber die Notwendigkeit, die Einwilligung nur auf einen oder mehrere konkret festgelegte Zwecke zu beschränken.

Nach Erwägungsgrund 33 Satz 1 DSGVO sollte es den Betroffenen „erlaubt sein, ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten **ethischen Standards** der wissenschaftlichen Forschung geschieht." Durch die Einhaltung der anerkannten ethischen Standards sollen die Risiken einer weiten Einwilligungserklärung in diesem Bereich aufgefangen werden. Diese Standards sind zwar nicht unmittelbar rechtsverbindlich, haben aber für die Konkretisierung der rechtlichen Anforderungen zumindest indizieller Wert. Ethische Standards ergeben sich in der Praxis aus Kodizes, Leitlinien und Erklärungen. Allerdings sind solche Standards die Verarbeitung personenbezogener Daten betreffend nicht in

allen Forschungsbereichen gleichermaßen etabliert. Aus der Zusammenarbeit von Forschenden mit Ethikkommissionen und Datenschutzbeauftragten ergibt sich die Möglichkeit, anhand praktischer Fälle auf die Entwicklung derartiger Standards hinzuarbeiten.

Nähere Informationen zu den forschungsethischen Grundsätzen und Standards in den Sozial- und Wirtschaftswissenschaften stellt der RatSWD in einem eigenen Output zur Verfügung (RatSWD 2017: 16 ff.)

Sofern ethische Standards etabliert sind und eingehalten werden, ist der „broad consent" eine wichtige Grundlage für eine Datenverarbeitung zu Forschungszwecken. Zu beachten ist aber, dass die Einwilligung auch in diesem Fall mit Wirkung für die Zukunft frei widerruflich bleibt.

Beispiel: Eine Einwilligung kann – mit Bezug auf bestimmte Daten oder eine zeitlich, sachlich oder räumlich begrenzte Datenerhebung – allgemein für die verhaltensökonomische Forschung oder einen ihrer Teilbereiche erteilt werden, ohne dass es im Ausgangspunkt einer näheren Zweckfestlegung bedarf.

Ungeschriebene Voraussetzung der Einwilligung ist, dass die- oder derjenige, der sie erteilt, **einsichtsfähig** ist. Auch Minderjährige können wirksam in eine Datenverarbeitung einwilligen, müssen die Konsequenzen ihrer Erklärung jedoch überblicken können. Eine feste Altersgrenze gibt es nicht, die Einsichtsfähigkeit ist individuell zu bestimmen. Regelmäßig dürfte sie zwischen Vollendung des 14. und 16. Lebensjahres vorliegen. Hiervon unabhängig kann eine Einwilligung von Erziehungsberechtigten bzw. des Vormundes notwendig sein.

Eine **schriftliche** Einwilligung ist nach der DSGVO nicht erforderlich, zumindest die Textform empfiehlt sich aber aus Nachweis- und Dokumentationsgründen. Die Textform erfordert im Unterschied zur Schriftform kein unterschriebenes Dokument, sondern nur eine Erklärung auf einem dauerhaften Datenträger, also etwa auf Papier oder in einem digitalen Format.

Weiter ist bei der Einwilligung zu beachten, dass diese von der betroffenen Person stets **widerrufen** werden kann (Art. 7 Abs. 3 DSGVO). Der Widerruf wirkt nur in die Zukunft, bisher zulässigerweise durchgeführte Datenverarbeitungen bleiben also zulässig. Ab dem Widerruf dürfen die betroffenen Daten jedoch nicht mehr auf Grundlage der Einwilligung weiterverarbeitet werden.

Die Widerruflichkeit der Einwilligung kann insbesondere bei Forschungsvorhaben, die auf längere Zeit angelegt sind (etwa Panelsurveys), missliche Konsequenzen haben. Bei solchen Vorhaben ist zu überlegen, sich von vornherein auf andere Rechtsgrundlagen als die Einwilligung zu stützen. Ist dies nicht möglich oder nicht gewünscht, so kann unter Umständen nach dem Widerruf einer Einwilligung die Datenverarbeitung noch auf eine andere Rechtsgrundlage gestützt werden. Hierauf sollten die Teilnehmenden bereits bei Einholung der Einwilligung hingewiesen werden, um keinen Vertrauenstatbestand zu schaffen, der den Rückgriff auf andere Rechtsgrundlagen sperrt.

Unberührt vom Widerruf einer Einwilligung bleibt die Weiterverarbeitung von ursprünglich personenbezogenen, zwischenzeitlich jedoch anonymisierten Daten. Diese Datenverarbeitung unterfällt mangels eines Personenbezugs schon nicht dem Anwendungsbereich des Datenschutzrechts. Eine bloße Pseudonymisierung ändert hingegen nichts daran, dass nach dem Widerruf die Daten nicht mehr verarbeitet werden dürfen, weil pseudonyme Daten gleichwohl personenbezogen sind.

Genauere Informationen zu den Voraussetzungen einer wirksamen Einwilligung stellt die Datenschutzaufsicht zur Verfügung (DSK 2019a).

5 Pflichten des Datenverarbeitenden

Im Folgenden sollen einige der zentralen Pflichten des forschenden Datenverarbeitenden vorgestellt werden.

5.1 Garantien für die Rechte und Freiheiten der Betroffenen

Wie bereits teilweise beschrieben, privilegiert die DSGVO an mehreren Stellen die Verarbeitung personenbezogener Daten zu Forschungszwecken. Quasi im Gegenzug legt sie forschenden Datenverarbeitenden allerdings auch die Pflicht auf, „**geeignete Garantien** für die Rechte und Freiheiten der betroffenen Person" vorzusehen, wie sich aus Artikel 89 Abs. 1 Satz 1 DSGVO ergibt.

Nach Art. 89 Abs. 1 Satz 2 DSGVO müssen die Garantien **technische und organisatorische Maßnahmen** enthalten, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung (vgl. 2.5) gewährleistet wird. Hierzu zählen unter anderem die Festlegung von Speicherfristen, Zugangsmöglichkeiten sowie das Gebot der Anonymisierung (vgl. 4.2) beziehungsweise Pseudonymisierung (4.3). Welche technisch-organisatorischen Maßnahmen im Detail geboten sind, hängt allerdings stark von dem konkreten Forschungsvorhaben ab. Es ist hier unter anderem zu berücksichtigen, welche personenbezogenen Daten verarbeitet werden und wer hieran beteiligt ist (Johannes und Richter 2017: 302).

Beispiel: Als organisatorische Maßnahme kann eine vertragliche Verpflichtung auf Einhaltung des Datenschutzes (Geheimhaltungsvereinbarung) vorgesehen werden, wie es bspw. die Forschungsdatenzentren mehrheitlich praktizieren. Auch der Auswahl des Datenzugangsweges (Download, Gastwissenschaftsarbeitsplatz, Remote Access) und dessen konkreter Ausgestaltung kommt eine besondere Bedeutung zu. Als technische Maßnahme kommt beispielsweise vor der Übermittlung von Daten eine Verschlüsselung in Betracht.

Neben Artikel 89 DSGVO verlangt auch § 27 Abs. 1 Satz 2 BDSG von dem Verantwortlichen angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person.[9] § 27 Abs. 3 Satz 1 BDSG sieht außerdem ein **Anonymisierungsgebot** für besondere Kategorien personenbezogener Daten vor, die zu Forschungszwecken verarbeitet werden. Dies ergibt sich allerdings bereits aus dem Anonymisierungsgebot in Art. 89 Abs. 1 Satz 4 DSGVO (vgl. oben 4.2).

5.2 Datensicherheit / Technische und organisatorische Maßnahmen

Wie bereits nach der alten Rechtslage sind nach Art. 32 DSGVO Datenverarbeitungsvorgänge technisch und organisatorisch abzusichern. Neben **physischen Sicherungen** wie abschließbaren Schränken und Brandschutz gehören dazu auch **IT-basierte Sicherungen** wie Verschlüsselungen und die Verwendung sicherer Dienste zur Datenspeicherung und zur Datenübermittlung. Grundsätzlich müssen sich die technischen Maßnahmen an dem „Stand der Technik" orientieren.

Hinsichtlich der für die Datenverarbeitung genutzten Dienste empfiehlt sich grundsätzlich die Verwendung von Lösungen, die **von der eigenen Forschungseinrichtung bereitgestellt** werden (vgl. zur Aufbewahrung von Forschungsdaten in Repositorien unten 9.1). Von externen Diensten ist abzuraten, speziell, wenn deren Nutzung mit Datenverarbeitungen außerhalb der Europäischen Union verbunden ist. Dies gilt explizit für Dropbox (Cloud), Onedrive (Cloud) und WhatsApp (Messenger). All diese Dienste werden von US-amerikanischen Anbietern zur Verfügung gestellt, deren Umgang mit Nutzerdaten nur eingeschränkt nachvollziehbar ist und gegenüber denen sich die Durchsetzung des Datenschutzrechts als besonders schwierig gestaltet.

9 Vgl. § 22 Abs. 2 Satz 2 BDSG.

5.3 Wahrung von Betroffenenrechten

Der Datenverarbeitende hat weiter die Rechte der betroffenen Personen zu wahren, die die DSGVO gegenüber der bisherigen Rechtslage erweitert hat. Hierbei ist zwischen transparenzschaffenden **Informationsrechten** (Art. 13-15 DSGVO) und **Einflussrechten** der betroffenen Personen auf die Datenverarbeitung (Art. 15-21 DSGVO) zu unterscheiden. Innerhalb der Informationsrechte muss zudem zwischen den proaktiv durch den Verantwortlichen zu erfüllenden Informationspflichten (Art. 13 und 14 DSGVO) und dem Auskunftsrecht (Art. 15 DSGVO), das einen Antrag der betroffenen Person voraussetzt, differenziert werden.

Für die **Informationspflichten** finden sich zwei unterschiedliche Regelungen. Art. 13 DSGVO regelt die Informationspflicht, wenn der Verantwortliche personenbezogene Daten bei der betroffenen Person erhebt (etwa durch eine Befragung der betroffenen Person oder eine Beobachtung ihres Verhaltens). Art. 14 DSGVO bezieht sich hingegen auf Datenerhebungen ohne Mitwirkung der betroffenen Person (etwa durch eine Befragung Dritter oder durch eine Recherche in öffentlich verfügbaren Quellen). Die Abgrenzung ist im Einzelnen komplex.

Beispiel: Werden Standortdaten mittels einer zu Forschungszwecken installierten App von einem Mobilfunkgerät erhoben, dient die betroffene Person selbst als Datenquelle und für die Informationspflicht gilt Art. 13 DSGVO. Werden Inhalts- oder Metadaten aus einem offen zugänglichen sozialen Netzwerk (z. B. Twitter) verarbeitet, erfolgt die Erhebung nicht direkt bei der betroffenen Person und Art. 14 DSGVO ist einschlägig.

Beide Regelungen stimmen hinsichtlich der Informationen, die der Verantwortliche der betroffenen Person zukommen lassen muss, weitgehend überein. Unterschiede bestehen hingegen zum einen hinsichtlich des Informationszeitpunkts: Die Informationspflicht des Art. 13 DSGVO ist zu Beginn der Datenerhebung zu erfüllen, während Art. 14 DSGVO eine spätere Information (spätestens innerhalb eines Monats) vorsieht. Zum anderen enthält Art. 14 DSGVO weitergehende **Ausnahmen** von der Informationspflicht. Insbesondere gilt bei Datenerhebungen ohne Mitwirkung der betroffenen Person gemäß Art. 14 Abs. 5 lit. b Halbsatz 2 DSGVO eine Ausnahme für wissenschaftliche Forschungszwecke. Eine Information ist danach nicht erforderlich, wenn sie die Ziele einer Datenverarbeitung für wissenschaftliche oder historische Forschungszwecke unmöglich macht oder ernsthaft beeinträchtigt. Diese Ausnahmeregelung ist von besonderer praktischer Relevanz, da sie eine aufwendige Pflicht der Forschenden ausschließen kann, die von ihrer Datenverarbeitung betroffenen Personen proaktiv zu informieren. Die Ausnahme greift allerdings nur dann, wenn Daten nicht direkt bei dem Betroffenen erhoben werden.

Beispiel: Bei massenhaften quantitativen Auswertungen von öffentlich zugänglichen personenbezogenen Daten, etwa aus sozialen Netzwerken im Internet, wird es oftmals praktisch nicht möglich sein, alle Betroffenen zu informieren. Zudem stünde zumindest bei nicht außergewöhnlich sensiblen Daten der Ertrag der Information für die betroffene Person in keinem ausgewogenen Verhältnis zu dem erforderlichen Aufwand, sie zu informieren. Die Informationspflicht aus Art. 14 DSGVO wird daher regelmäßig nicht greifen.

Die Datenschutzbehörden stellen genauere Informationen zu der Wahrung der Informationspflichten zur Verfügung (zum Beispiel DSK 2018e, ULD 2019a).

Die betroffene Person hat daneben nach Art. 15 DSGVO ein **Auskunftsrecht**, das ein Recht auf Übermittlung einer Kopie der über sie gespeicherten Daten einschließt. Die DSGVO enthält für dieses Auskunftsrecht keine Ausnahme, die für die wissenschaftliche Forschung relevant wäre. Eine Ausnahmeregelung findet sich jedoch in § 27 Abs. 2 Satz 2 BDSG. Danach ist das Auskunftsrecht für die Fälle eingeschränkt, dass die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde. Die forschungsrelevanten Einflussrechte der betroffenen Person umfassen die Rechte auf Berichtigung unrichtiger Daten (Art. 16 DSGVO), auf Löschung rechtswidrig verarbeiteter oder nicht mehr benötigter Daten (Art. 17 DSGVO – sogenanntes Recht auf Vergessenwerden) und auf Einschränkung der Verarbeitung insbesondere in Zweifelsfällen (Art. 18 DSGVO). In besonders gelagerten Fällen kann eine betroffene Person einer Datenverarbeitung zudem widersprechen (Art. 21 DSGVO).

Orientierungshilfen zum praktischen Vollzug des Auskunftsrechts (DSK 2018d) und des Rechts auf Löschung (DSK 2018f) bieten die Datenschutzbehörden.

Die DSGVO und die nationalen Datenschutzgesetze enthalten Ausnahmeregelungen von diesen Einflussrechten zum Schutz der Wissenschaftsfreiheit. Insgesamt sind diese Ausnahmen weitgehend und erlauben es in der Regel, die Betroffenenrechte einzuschränken, wenn sich durch deren Verwirklichung Forschung nicht verwirklichen ließe.

Für das **Recht auf Vergessenwerden** nach Art. 17 DSGVO regelt Abs. 3 lit. d der Vorschrift eine Ausnahme. Diese greift, wenn die Datenverarbeitung für wissenschaftliche Forschungszwecke erforderlich ist, soweit das Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder diese ernsthaft beeinträchtigen würde.

Aus Art. 21 Abs. 6 DSGVO ergibt sich für das **Widerspruchsrecht** eine Privilegierung für wissenschaftliche Forschungszwecke. Eine wissenschaftliche Datenverarbeitung kann trotz Widerspruchs fortgesetzt werden, wenn die Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist. Das Widerspruchsrecht ist nach § 27 Abs. 2 Satz 1 BDSG ebenso wie die Rechte auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO) und Einschränkung der Verarbeitung (Art. 18 DSGVO) eingeschränkt, wenn durch sie der Forschungszweck unmöglich gemacht oder ernsthaft beeinträchtigt würde. Die vorgenommenen Abwägungen sind zu dokumentieren.

5.4 Führen eines Verfahrensverzeichnisses

Die DSGVO verpflichtet den für die Datenverarbeitung Verantwortlichen, ein Verzeichnis über seine Verarbeitungstätigkeiten zu führen (Art. 30 DSGVO). Dieses Verzeichnis dient der Bestandsaufnahme über die laufenden Arbeiten mit personenbezogenen Daten. Es ist auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen (§ 30 Abs. 4 DSGVO). Die Pflicht, ein Verfahrensverzeichnis zu führen, lässt sich als Ausdruck der allgemeinen Rechenschaftspflicht des Verantwortlichen verstehen (Art. 5 Abs. 2 DSGVO). Dieser ist dazu verpflichtet, die Einhaltung datenschutzrechtlicher Grundsätze nachweisen zu können.

Nähere Informationen (DSK 2018, DSK 2018a) und Muster (DSK 2018b) zur Führung von Verfahrensverzeichnissen stellen die Datenschutzaufsichtsbehörden zur Verfügung.

5.5 Bestellung eines Datenschutzbeauftragten

Des Weiteren haben Datenverarbeitende nach Art. 37 DSGVO eigene Datenschutzbeauftragte zu benennen. Diese Pflicht trifft grundsätzlich **öffentliche Stellen** sowie **nicht-öffentliche Stellen**, die in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen oder besonders riskante Datenverarbeitungen durchführen (Art. 37 Abs. 1 DSGVO, § 38 BDSG).

Zu den Aufgaben der Datenschutzbeauftragten gehört es, die Datenverarbeitenden hinsichtlich ihrer Pflichten nach der DSGVO zu **unterrichten** und zu **beraten** sowie die Einhaltung dieser zu **überwachen** (Art. 39 Abs. 1 DSGVO).

Die Datenschutzbeauftragten von Forschungseinrichtungen sind wichtige Ansprechpartner für Anwendungsfragen der DSGVO. Sie sollten bei der Planung und Ausführung von Forschungsvorhaben, die die Verarbeitung personenbezogener Daten erfordern, **konsultiert** werden. Datenschutzkonzepte sollten mit ihnen abgestimmt werden.

Die Aufsichtsbehörden stellen genauere Informationen zu der Bestellung sowie den Rechten und Pflichten von Datenschutzbeauftragten zur Verfügung (DSK 2018g, ULD 2019).

5.6 Durchführung einer Datenschutz-Folgenabschätzung

Für besonders riskante Datenverarbeitungen verpflichtet die DSGVO zur Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO). Sie kann beispielsweise nötig werden, wenn in einem Forschungsprojekt umfangreich **besondere Kategorien**[10] **personenbezogener Daten** (Art. 9 DSGVO, vgl. 4.1) verarbeitet werden – so etwa Gesundheitsdaten oder Daten über Religionszugehörigkeiten.

Inhaltlich erfordert die Datenschutzfolgenabschätzung unter anderem die Beschreibung der Verarbeitungsvorgänge und -zwecke sowie die Bewertung der vorliegenden Risiken und geplanten Abhilfemaßnahmen (Art. 35 Abs. 7 DSGVO). Praktisch existieren zu der Durchführung der Datenschutz-Folgenabschätzung noch keine ausführlichen Erfahrungswerte, da es sich um ein neues Instrument der DSGVO handelt.

Papiere der Datenschutzkonferenz bieten eine Orientierungshilfe, in welchen Fällen (LDA Brandenburg 2018) und wie (DSK 2018c) Datenschutz-Folgenabschätzungen durchzuführen sind.

Auf Anfrage ist die oder der **Datenschutzbeauftragte** der Institution in den Vorgang mit einzubeziehen (Art. 39 Abs. 1 lit. c DSGVO). Auch die zuständige **Aufsichtsbehörde** kann nach Art. 36 DSGVO mit einzubeziehen sein, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

10 Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten und Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

6 Datenakquise (bei der Feldarbeit)

Der folgende Abschnitt konzentriert sich auf die erstmalige Erhebung personenbezogener Daten durch Forschende (**Primärdatenerhebungen**). Vor der erstmaligen Erhebung sollte der Forschungszweck möglichst genau definiert und geprüft werden, welche Daten hierfür notwendig sind (im Sinne des Prinzips der Datenminimierung). Bereits im Vorfeld der Erhebung sollte auch ein Konzept vorhanden sein, wie die erhobenen Daten in der Folge gespeichert, aufbewahrt (vgl. 9) und technisch-organisatorisch geschützt werden (vgl. 5.1 und 5.2) sollen. Hierbei ist ggf. auch die oder der Datenschutzbeauftragte der Forschungsinstitution heranzuziehen.

Als Rechtsgrundlage für die Datenverarbeitung kommt entweder eine Einwilligung oder eine gesetzliche Erlaubnis in Betracht.

6.1 Auf Grundlage einer Einwilligung

Bei der Datenerhebung auf Grundlage einer Einwilligung ist zunächst sicherzustellen, dass die Einwilligung **informiert und bestimmt** erfolgt (vgl. 4.5). Dabei sollte die geplante und mögliche Verwendung der Daten vorausschauend möglichst umfassend beschrieben werden, da sie auf Grundlage der Einwilligung an die hierin beschriebenen Zwecke gebunden bleibt. Auch eine möglicherweise geplante und notwendige Weitergabe von Daten an Forschungspartner, Repositorien und andere Stellen zum Zwecke der gemeinsamen Bearbeitung, einer Archivierung bzw. Nachnutzung oder einer Veröffentlichung in anonymisierter Form ist bereits in der Einwilligung zu verankern.

Auf die **Freiwilligkeit** der Teilnahme an einer Datenerhebung ist ebenso hinzuweisen wie auf die Möglichkeit des Widerrufs der Einwilligung. Personen, die die Teilnahme verweigern, dürfen weder Nachteile entstehen, noch darf Druck zur Teilnahme ausgeübt werden.

Sollen Daten nicht nur über den Befragten selbst, sondern auch **über Dritte** (beispielsweise bei einer Befragung über Ehepartner oder Kinder des Befragten) erhoben werden, reicht die Einwilligung des Befragten als Grundlage hierfür nicht aus.[11] Es ist entweder eine Einwilligung der Dritten einzuholen oder eine gesetzliche Grundlage für die Verarbeitung heranzuziehen (vgl. 6.2).

Wenn eine **Wiederholungsbefragung** geplant ist, sollten die Betroffenen darüber informiert werden. Damit sie erneut kontaktiert werden können, sollte sich die Einwilligung auch auf die Speicherung ihrer Kontaktdaten für diesen Zweck beziehen.

Sollen in einem **„record linkage“** Verfahren, also mittels Verknüpfung verschiedener Datenquellen zu ein und derselben Person, neue Daten verarbeitet werden, ist dies in der Einwilligungserklärung gesondert anzuführen.

Einwilligungserklärungen können sich neben den direkt aus einer Befragung gewonnenen Daten auch auf weitere Daten beziehen, die während des Erhebungsprozesses anfallen (**Paradaten**). Diese betreffen zum Beispiel die Art und Anzahl der Kontaktierungen, die Dauer der Beantwortung einzelner Fragen (bei computerassistierten Datenerhebungssystemen), Sprachtempo oder andere Merkmale eines Interviews. Diese Daten können unter anderem zur Qualitätssicherung einer Studie eingesetzt werden. Eine Einwilligung bzgl. der Paradaten ist möglich, wenn diese in der Erklärung hinreichend deutlich bezeichnet werden.

11 Zwar ist nicht endgültig geklärt, ob die Einwilligung im Datenschutzrecht stets höchstpersönlich erfolgen muss, es wäre aber jedenfalls eine wirksame Stellvertretung erforderlich, damit ein Befragter für Dritte einwilligen kann.

Die Erteilung der Einwilligung sollte zu Beweiszwecken zumindest in Textform **dokumentiert** werden, auch wenn diese Form für ihre Wirksamkeit nicht notwendig ist (vgl. 4.5). Diese Dokumentation sollte mindestens solange aufbewahrt werden, wie die Datenverarbeitung erfolgt. Wird eine wirksame Einwilligung eingeholt, besteht hierdurch zunächst Rechtssicherheit für die Verarbeitung der Forschungsdaten. Es ist allerdings zu beachten, dass dem Betroffenen jederzeit das Recht bleibt, die Einwilligung mit Wirkung für die Zukunft zu **widerrufen**.

6.2 Auf gesetzlicher Grundlage

Die Datenakquise kann nicht nur auf Grundlage einer Einwilligung, sondern auch auf gesetzlicher Grundlage erfolgen. Hierfür gelten die allgemeinen Erlaubnistatbestände der DSGVO: Während öffentliche Stellen sich auf die **Erfüllung ihrer Aufgaben** berufen können (Art. 6 Abs. 1 lit. e DSGVO), kommt für private Datenverarbeitende vor allem die Erhebung aufgrund **überwiegender Interessen** in Betracht (Art. 6 Abs. 1 lit. f DSGVO). Bei der Erhebung besonderer personenbezogener Daten ist zusätzlich Art. 9 DSGVO zu beachten (vgl. 4.1).

Die Einwilligung genießt **keinen grundsätzlichen Vorrang** gegenüber den übrigen Erlaubnistatbeständen. Eine Datenerhebung auf gesetzlicher Grundlage kann unter Umständen praktikabler sein als die Erteilung einer Einwilligung. Das gilt etwa dann, wenn Daten nicht direkt durch eine Befragung erhoben werden, sondern zum Beispiel aus Drittquellen. Auch für die Verarbeitung von Paradaten (Daten, die neben direkt aus einer Befragung gewonnenen Daten während des Erhebungsprozesses anfallen) kommen gesetzliche Grundlagen in Betracht.

Gegenüber der Erhebung auf Basis einer Einwilligung hat die Erhebung und Verarbeitung auf Grundlage einer gesetzlichen Erlaubnis den Vorteil, dass der Betroffene kein voraussetzungsloses Recht zum Widerruf hat. Er kann der Datenverarbeitung allerdings unter Umständen aus besonderen Gründen **widersprechen** (Art. 21 DSGVO). Zu beachten ist auch, dass die Einholung einer Einwilligung den Rückgriff auf eine gesetzliche Erlaubnis versperren kann, wenn der Betroffene darauf vertraut, dass seine Daten nur auf Grundlage und im Rahmen der Einwilligung verarbeitet werden. Wenn überhaupt eine Einwilligung erwünscht ist oder eingeholt werden muss, so kann deshalb ein Hinweis darauf sinnvoll sein, dass die Daten nach einem Wegfall der Einwilligung ggfs. auf anderer Grundlage weiterverarbeitet werden können.

Beispiel: Eine Forscherin bittet eine Interviewpartnerin um Erteilung einer Einwilligung zur Verarbeitung der in dem Interview erhobenen Informationen für ihr Forschungsprojekt. Sie sagt der Interviewpartnerin, die Informationen würden nur mit ihrem Einverständnis verarbeitet. Zwei Wochen nach dem Interview entscheidet sich die Interviewpartnerin dafür, ihre Einwilligung zu widerrufen, da ihr ihre Aussagen im Nachhinein unangenehm sind. Die Forscherin kann die Informationen nun nicht auf Grundlage von Art. 6 Abs. 1 lit. e oder f DSGVO (öffentliche Aufgabe bzw. berechtigte Interessen) auswerten, da sie sonst das schutzwürdige Vertrauen der Interviewpartnerin brechen würde.

7 Datenaufbereitung und Datenanalyse (nach der Feldarbeit)

Die Aufbereitung und Analyse der Daten sind **neue Verarbeitungsschritte**, die ebenfalls einer Rechtfertigung bedürfen. Soweit die Aufbereitung und Analyse demselben Forschungszweck wie die Datenerhebung dienen, wird allerdings der Erlaubnistatbestand, auf dem die Datenerhebung beruht, in der Regel auch die nachgelagerten Verarbeitungsschritte erlauben. Probleme können entstehen, wenn auf der Analyseebene neue Methoden oder Erkenntnisziele hinzukommen, die sich zwar noch im Rahmen des Forschungszwecks halten, aber die Betroffenen besonders stark belasten. In solchen Fällen kann es erforderlich sein, eine neue Interessenabwägung durchzuführen oder eine zusätzliche Einwilligung einzuholen.

Beispiel: Im Rahmen eines langfristig angelegten Forschungsprojekts zum Wandel weltanschaulicher Überzeugungen werden die Probandinnen und Probanden in regelmäßigen Abstand zu zeitpolitischen Themen befragt. Nach einiger Zeit stellt sich heraus, dass die Antworten nicht nur in aggregierter Form allgemeine Aussagen ermöglichen, sondern mit ihrer Hilfe – etwa durch neue komplexe Auswertungsmethoden oder durch eine Verknüpfung mit weiteren verfügbaren personenbezogenen Datenbeständen – auch individuelle Radikalisierungsprozesse prognostiziert werden können. Dieses neue Erkenntnisziel mag man noch als von dem ursprünglichen Forschungszweck gedeckt ansehen. Aufgrund der Auswertungstiefe und -breite sowie des potenziell stigmatisierenden Erkenntnisziels wird eine solche Datenanalyse jedoch nicht mehr ohne weiteres durch die Einwilligung oder die Interessenabwägung gedeckt, welche die Datenerhebungen und die zuvor vorgenommenen, weniger sensiblen Analysen gerechtfertigt haben. Es ist vielmehr neu und eigenständig zu prüfen, ob ein gesetzlicher Erlaubnistatbestand vorliegt bzw. eine Einwilligung eingeholt werden muss.

In der Phase der Datenaufbereitung sind geeignete **technische und organisatorische Maßnahmen** zu treffen, um den Schutz der betroffenen Personen zu gewährleisten (vgl. 5.1 und 5.2). Die Daten müssen frühestmöglich pseudonymisiert werden. Nach Abschluss der Datenaufbereitung ist zu prüfen, inwiefern Bruttodaten (d. h. inkl. Metadaten) und Kontaktdaten zur weiteren Nachvollziehbarkeit oder aus sonstigen Gründen (z. B. Panel) einer weiteren Aufbewahrung bedürfen. Ansonsten müssen sie, sobald es der Forschungszweck erlaubt, anonymisiert werden (Art. 89 Abs. 1 Satz 4 DSGVO, § 27 Abs. 3 Satz 1 BDSG). Sofern den von der Datenverarbeitung Betroffenen eine Löschung der Daten innerhalb eines bestimmten Zeitraums zugesagt wurde, ist diese vorzunehmen.

8 (Daten-)Publikation

Auch die Publikation personenbezogener Daten ist eine Form der Datenverarbeitung (vgl. 2.1), die einer eigenen Rechtfertigung bedarf. Hierunter kann beispielsweise die wissenschaftliche Diskussion von Verhaltensweisen, Lebensläufen oder Krankheiten einzelner identifizierbarer Personen fallen. Auch sobald Daten beispielsweise in Journals oder auch in Repositorien zur Reanalyse zugänglich gemacht werden, handelt es sich um eine Publikation von Daten. Die Publikation von Daten ist – sofern die Daten noch personenbeziehbar (also nicht anonym) sind – mit einer Einwilligung zu rechtfertigen (§ 27 Abs. 4 BDSG).

Die Publikation führt dazu, dass Informationen einem potentiell unbegrenzten Personenkreis zugänglich werden und bedeutet daher einen **besonders intensiven Eingriff** in die Rechte der betroffenen Person. Aus datenschutzrechtlicher Sicht ist besondere Vorsicht geboten. Soweit dies ohne Beeinträchtigung des Forschungszwecks und ohne Verfälschung der Forschungsergebnisse möglich ist, müssen die im Rahmen der Forschungsarbeit gewonnenen Ergebnisse für die Veröffentlichung so aufbereitet werden, dass ein Personenbezug nicht mehr möglich ist (Anonymisierung, vgl. 4.2).

Bei der Veröffentlichung quantitativer Daten wird die wirksame Anonymisierung dabei deutlich leichter fallen als bei qualitativen Daten, da nicht die Daten als solche, sondern nur die Analyseergebnisse veröffentlicht werden. Bei einer qualitativen Datenanalyse kann die Identifikation einzelner Betroffener aufgrund spezifischer Merkmale – wie beispielswiese des individuellen Sprach- oder Schreibstils einer Person (vgl. Winter/Battis/Halvani 2019: 491 f.) – möglich sein, die sich nicht leicht tilgen lassen, ohne die Aussagekraft einer Publikation zu schwächen. Der Ausgleich der gegenläufigen Anliegen eines wirksamen Datenschutzes durch Anonymisierung einerseits und der Wahrung der wissenschaftlichen Genauigkeit andererseits erweist sich speziell in diesem Fall als Gratwanderung.

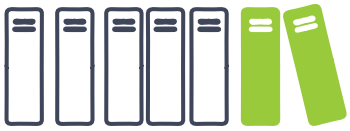
Beispiel: Eine Dialektologin veröffentlicht Ausschnitte aus Interviews mit Sprechern seltener Mundarten. Aufgrund der individuellen Sprachstile und der Gegenstände der Interviews sind Rückschlüsse auf die sprechenden Personen möglich.

Eine spezielle Regelung für die **Veröffentlichung besonderer Kategorien personenbezogener Daten** (vgl. 4.1) zu Forschungszwecken trifft § 27 Abs. 4 BDSG. Voraussetzung für eine Veröffentlichung ist demnach, dass die betroffene Person eingewilligt hat (vgl. 4.5) oder dass die personenbezogene Veröffentlichung für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

Um zu beurteilen, ob eine Veröffentlichung personenbezogener Daten **zur zeitgeschichtlichen Darstellung unerlässlich** ist, sind die historischen Forschungsinteressen und die Interessen am Schutz der Persönlichkeitsrechte gegeneinander abzuwägen. Es ist zu prüfen, welchen Informationswert personenbezogene Daten in Bezug auf das relevante Ereignis der Zeitgeschichte haben.

Bedauerlicherweise ist die Ausnahmeregelung in § 27 Abs. 4 BDSG mit ihrem Fokus auf die Zeitgeschichte recht eng geraten. Sie erschwert im Zusammenwirken mit Art. 9 DSGVO Veröffentlichungen, die einerseits nicht ohne sensible Daten auskommen und bei denen sich andererseits ein Personenbezug nicht ausschließen lässt (etwa eine – auch nur partielle – Wiedergabe von Interviews über politische Haltungen oder die Bewältigung der individuellen Krankengeschichte, wenn daraus mit entsprechendem Zusatzwissen Rückschlüsse auf den Interviewpartner gezogen werden können). Bei derartigen Forschungsprojekten verbleibt zur Gewährleistung einer rechtskonformen Publikation von Forschungsergebnissen nur die Einwilligung, die von vornherein auch die Veröffentlichung in pseudonymisierter Form umfassen sollte.

Die Veröffentlichung **sonstiger personenbezogener** Daten richtet sich nach der allgemeinen Regelung in Art. 6 DSGVO. Sie kann ebenfalls auf Grundlage einer Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) oder im Rahmen der öffentlichen Aufgabe bzw. aufgrund überwiegender Interessen (Art. 6 Abs. 1 lit. e und f DSGVO) erfolgen. Bei der Interessenabwägung ist zu beachten, dass die Veröffentlichung einen verhältnismäßig tiefen Eingriff für den Betroffenen bedeutet. Dennoch lassen Art. 6 Abs. 1 lit. e und f DSGVO einen wesentlich größeren Spielraum für die Veröffentlichung personenbezogener Daten als Art. 9 DSGVO und § 27 Abs. 4 BDSG.



9 Aufbewahrung und sekundäre Nutzung von Forschungsdaten

9.1 Aufbewahrung und Archivierung

Nach Abschluss eines Forschungsprojekts stellen sich datenschutzrechtliche Fragen im Zusammenhang mit der weiteren Aufbewahrung der angefallenen personenbezogenen Daten. Die Regeln **guter wissenschaftlicher Praxis** sehen vor, Forschungsdaten nach Projektabschluss aufzubewahren – nach den Leitlinien der DFG beispielsweise für einen Zeitraum von in der Regel zehn Jahren (DFG 2019: 22).

Für die Speicherung ist allerdings eine Rechtsgrundlage erforderlich, sofern die Daten weiter einen Personenbezug aufweisen. Dies sollte ggfs. schon bei der **Einwilligung**, die bei der Erhebung erteilt wird, mitbedacht werden, wobei auf die Aufbewahrung unter Nennung einer Höchstspeicherfrist hinzuweisen ist. Ansonsten kommen die **gesetzlichen Erlaubnisse** in Betracht. Eine Aufbewahrung zur Dokumentation der Forschung wird von den Forschungsaufgaben öffentlicher Institutionen regelmäßig gedeckt sein. Für private Forschungsinteressen wird es im Rahmen einer Interessenabwägung unter anderem darauf ankommen, ob besondere Interessen der Betroffenen gegen eine längere Aufbewahrung sprechen.

Im Übrigen sind auch im Rahmen der Archivierung **technische und organisatorische Maßnahmen** zum Schutz der Daten vor missbräuchlichem Zugriff sowie zum Schutz ihrer Integrität unerlässlich und stetig zu aktualisieren.

In der Praxis bieten sich für die Aufbewahrung von Forschungsdaten Repositorien und Forschungsdatenzentren innerhalb oder außerhalb der eigenen Einrichtung an. Bei der Auswahl von Repositorien und Forschungsdatenzentren sollten Aspekte von Datenschutz und Datensicherheit mit einbezogen werden.

Ausführliche praxisorientierte Hinweise zu Archivierung und Repositorien finden sich in der Orientierungshilfe des RatSWD zu Forschungsdatenmanagement in den Sozial-, Verhaltens- und Wirtschaftswissenschaften (RatSWD 2018). Aktuelle zusammenfassende Informationen zum Datenschutz bei den vom RatSWD akkreditierten Forschungsdatenzentren finden sich in ihrem Tätigkeitsbericht für das Jahr 2018 (RatSWD 2019: 33 ff.).

9.2 Sekundäre Nutzung

Schließlich stellt sich regelmäßig die Frage, unter welchen Bedingungen aufbewahrte (pseudonymisierte) Forschungsdaten für neue Forschungsprojekte verwendet werden dürfen. Die Verarbeitung auf Grundlage einer Einwilligung oder gesetzlichen Erlaubnis ist zunächst auf die zu Beginn der Verarbeitung festgelegten Zwecke beschränkt (**Zweckbindung**).

Es ist jedoch möglich, die Daten auf einer neuen rechtlichen Grundlage weiterzuverarbeiten. Nach Art. 5 Abs. 1 lit. b Halbsatz 2 DSGVO gilt eine Weiterverarbeitung von Daten für wissenschaftliche Zwecke, die ursprünglich für andere Zwecke erhoben wurden, nicht als unvereinbar mit den ursprünglichen Zwecken. Demnach darf die Weiterverarbeitung erfolgen, wenn die Voraussetzungen einer Rechtsgrundlage hierfür vorliegen – diese können sich aus der **gleichen Rechtsnorm** ergeben wie bei der ursprünglichen Verarbeitung.

Beispeil: Forscherinnen haben auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO Daten aus sozialen Netzwerken in Form von inhaltlichen Beiträgen und Interaktionen erhoben, um Erkenntnisse über sprachspezifische Besonderheiten der Nutzerinnen in den jeweiligen Netzwerken zu gewinnen. Nun möchten andere Forscherinnen anhand dieser Daten die gruppenspezifische Diskussionskultur in den sozialen Medien untersuchen. Sie können sich auch dafür auf Art. 6 Abs. 1 lit. f DSGVO stützen, wobei die Interessenabwägung neu vorzunehmen ist. Hingegen bedarf es keiner besonderen Erlaubnis für die Zweckänderung, die in der Datennutzung für den neuen Forschungszweck liegt.

10 Checklisten und Best Practices

Die folgenden Checklisten und Stichpunkte sollen einen möglichst knappen Überblick über wichtige Aspekte geben, die bei der Verarbeitung personenbezogener Daten zu Forschungszwecken zu beachten sind. Sie erheben **keinen Anspruch auf Vollständigkeit** und sind im Zusammenhang mit den vorigen Ausführungen der Handreichung zu lesen.

10.1 Grundlegende Fragen bei der Datenverarbeitung

- Werden personenbezogene Daten verarbeitet?
  - Definition in Art. 4 Nr. 1 DSGVO. Kein Personenbezug bei wirksamer Anonymisierung.
  - Jede Verarbeitung bedarf einer Rechtfertigung nach Art. 6 Abs. 1 DSGVO: Einwilligung oder gesetzliche Erlaubnis.
- Handelt es sich um besondere personenbezogene Daten (Art. 9 DSGVO)?
  - Aufgezählt in Art. 9 Abs. 1 DSGVO und näher definiert in Art. 4 Nr. 13 ff. DSGVO.
  - Wenn ja, bedarf es neben Art. 6 Abs. 1 DSGVO einer zusätzlichen Rechtfertigung nach Art. 9 Abs. 2 DSGVO.
- Sind technisch-organisatorische Schutzmaßnahmen für die Datenverarbeitung getroffen?
  - Hierzu gehören Maßnahmen zum Schutz vor Vernichtung, Veränderung, Verlust und Offenlegung von Daten, die dem aktuellen Stand der Technik entsprechen.
  - Physische Sicherheitsvorkehrungen, technische Sicherungen virtueller Speicher, Schulung der Mitarbeiterinnen, schriftliche Vereinbarungen (Nutzungsverträge), Rechtemanagement.
- Ist eine Datenschutzfolgenabschätzung vorzunehmen?

Für jeden Verarbeitungsschritt ist zu prüfen:

- Für öffentliche Stellen: Ist die Datenverarbeitung zur Erfüllung einer Forschungsaufgabe erforderlich?
- Für nicht-öffentliche Stellen: Ist die Datenverarbeitung zur Wahrung eines Forschungsinteresses erforderlich, dem keine überwiegenden Interessen der Betroffenen entgegenstehen?
- ODER: Liegt eine wirksame (freiwillige) Einwilligung vor (Art. 4 Nr. 11 DSGVO)?
- Gibt es wichtige Interessen, die trotzdem gegen die Verarbeitung sprechen könnten?
- Könnte die Aufgabe auch mit weniger Daten erfüllt werden?
- Könnte sie mit anonymen/pseudonymen Daten erfüllt werden?

10.2 Weitere Überlegungen

- Wie werden die Daten aufbewahrt?
  - Es sind sichere Aufbewahrungslösungen zu wählen, die Verlust der Daten und unbefugten Zugriff möglichst ausschließen.
- Wer hat Zugang zu den Daten? (Forschungsteam, ggf. Hiwis, Sekretariat)
  - Der Kreis der Zugangsberechtigten ist auf diejenigen zu beschränken, die notwendigerweise mit diesen Daten arbeiten müssen.

- Wie lange werden die Daten aufbewahrt?
  - Es sollte in jedem Fall eine maximale Speicherfrist festgelegt werden.
- Wurden die Betroffenen über die Datenverarbeitung informiert?
  - Die Informationspflichten ergeben sich aus Art. 13 und Art. 14 DSGVO und sind im Einzelfall zu prüfen.
- Gibt es die Möglichkeit des Widerspruchs gegen die Datenverarbeitung (Löschung)?
  - Diese Möglichkeit ist in jedem Fall einzuräumen.
- Werden die Daten an Dritte weitergeleitet? Wenn ja, an wen? Auch an Dritte außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums?
  - Die Übermittlung ist als eigenständiger Verarbeitungsschritt auf ihre Rechtmäßigkeit zu prüfen. Die Übermittlung in Drittländer erfordert eine gesonderte Prüfung nach Art. 44 ff. DSGVO (vgl. DSK 2019).

10.3 Best Practices

- Die Forschungsfrage sowie die Methodik eines Forschungsprojektes sind in einem Forschungsdesign festzuhalten, das seinem Inhalt und seinem Vorgehen nach wissenschaftlichen Ansprüchen genügt. Dabei sollte dargestellt werden, welche Arten von personenbezogenen Daten in welchem Umfang und mittels welcher technischen Ansätze erhoben, verarbeitet und gespeichert werden.
- Der oder die Datenschutzbeauftragte der eigenen Institution sollte frühzeitig in das Projekt eingebunden und im Laufe des Projektes über etwaige Änderungen des Forschungsdesigns oder Ähnliches unterrichtet werden.
- Die dargestellten Rechtsgrundlagen der Datenverarbeitung sollten für das Vorhaben geprüft werden. Dazu gehört auch die Prüfung der Möglichkeit einer Einwilligung, auch wenn diese keinen Vorrang vor anderen Varianten der Rechtfertigung hat. Es sollte dokumentiert werden, warum welche Rechtsgrundlage für die geplante Datenverarbeitung für einschlägig gehalten wird. Bei einer Interessenabwägung sollten die wesentlichen Kriterien festgehalten werden.
- Das erhobene Datenmaterial ist regelmäßig auf seine Qualität, Sicherung und Notwendigkeit zu überprüfen.
- Es sollten technische und organisatorische Maßnahmen zum Datenschutz getroffen werden. Hierzu zählen – ohne einen Anspruch auf Vollständigkeit – Vorkehrungen zur Datenminimierung, die Nutzung von Anonymisierungs- beziehungsweise Pseudonymisierungsmöglichkeiten, die Festlegung von Speicherfristen sowie deren Befolgung, die Löschung unbrauchbarer oder obsoleter Daten, die Implementierung von Rollenkonzepten sowie Secure Access-Lösungen. Es sind Sicherungsmechanismen vorzusehen, um die Abschöpfung oder Manipulation des Datenmaterials zu verhindern.
- Um die Betroffenenrechte erfüllen zu können, sind passende technische und organisatorische Rahmenbedingungen zu schaffen, etwa durch die Ordnung der Datensätze.
- Die Forschungsergebnisse sowie die zugrundeliegenden Datenstämme sind langfristig datenschutzfreundlich zu archivieren, soweit sie zur Nachvollziehbarkeit der Forschung oder weitere Vorhaben weiterhin benötigt werden.
- Forschungsergebnisse sind datenschutzfreundlich zu kommunizieren. Dabei sind besonders moderne technische Möglichkeiten zu beachten, aus scheinbar unverfänglichen Informationen Personenbezüge herzustellen.

11 Literaturverzeichnis

Albrecht, Jan Philipp und Florian Jotzo (2017): Das neue Datenschutzrecht der EU. Baden-Baden, Nomos.

Arning, Marian; Nikolaus Forgó und Tina Krügel (2006): Datenschutzrechtliche Aspekte der Forschung mit genetischen Daten. Datenschutz und Datensicherheit 30(11), 700–705.

DFG [Deutsche Forschungsgemeinschaft] (2019): Leitlinien zur Sicherung guter wissenschaftlicher Praxis. Kodex. https://www.dfg.de/download/pdf/foerderung/rechtliche_rahmenbedingungen/gute_wissenschaftliche_praxis/kodex_gwp.pdf (Zugriff am 21.12.2019).

DSK [Datenschutzkonferenz] (2018): Kurzpapier Nr. 1. Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO. Stand: 17.12.2018. https://www.datenschutzkonferenz-online.de/kurzpapiere.html (Zugriff am 21.12.2019).

DSK [Datenschutzkonferenz] (2018a): Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO. https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf (Zugriff am 21.12.2019).

DSK [Datenschutzkonferenz] (2018b): Muster für Verantwortliche gemäß Artikel 30 Abs. 1 DSGVO. https://www.datenschutzkonferenz-online.de/anwendungshinweise.html (Zugriff am 21.12.2019).

DSK [Datenschutzkonferenz] (2018c): Kurzpapier Nr. 5. Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO. Stand: 17.12.2018. https://www.datenschutzkonferenz-online.de/kurzpapiere.html (Zugriff am 21.12.2019).

DSK [Datenschutzkonferenz] (2018d): Kurzpapier Nr. 6. Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO. Stand: 17.12.2018. verfügbar unter https://www.datenschutzkonferenz-online.de/kurzpapiere.html (Zugriff am 21.12.2019).

DSK [Datenschutzkonferenz] (2018e): Kurzpapier Nr. 10. Informationspflichten bei Dritt- und Direkterhebung. Stand: 16.01.2018. https://www.datenschutzkonferenz-online.de/kurzpapiere.html (Zugriff am 21.12.2019).

DSK [Datenschutzkonferenz] (2018f): Kurzpapier Nr. 11. Recht auf Löschung / „Recht auf Vergessenwerden". Stand: 17.12.2018. https://www.datenschutzkonferenz-online.de/kurzpapiere.html (Zugriff am 21.12.2019).

DSK [Datenschutzkonferenz] (2018g): Kurzpapier Nr. 12. Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern. Stand: 17.12.2018. https://www.datenschutzkonferenz-online.de/kurzpapiere.html (Zugriff am 21.12.2019).

DSK [Datenschutzkonferenz] (2018h): Kurzpapier Nr. 17. Besondere Kategorien personenbezogener Daten. Stand: 27.03.2018. https://www.datenschutzkonferenz-online.de/kurzpapiere.html (Zugriff am 21.12.2019).

DSK [Datenschutzkonferenz] (2019): Kurzpapier Nr. 4. Datenübermittlung in Drittländer. Stand: 22.07.2019. https://www.datenschutzkonferenz-online.de/kurzpapiere.html (Zugriff am 21.12.2019).

DSK [Datenschutzkonferenz] (2019a): Kurzpapier Nr. 20. Einwilligung nach der DS-GVO. Stand: 22.02.2019. https://www.datenschutzkonferenz-online.de/kurzpapiere.html (Zugriff am 21.12.2019).

Golla, Sebastian; Henning Hofmann und Matthias Bäcker (2018): Connecting the Dots – Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DS-GVO und BDSG-neu. Datenschutz und Datensicherheit 42(2), 89–100.

Golla, Sebastian (2019): Datenschutz in der Forschung und Hochschullehre. In: Louisa Specht und Reto Mantz (Hrsg.): Handbuch Europäisches und deutsches Datenschutzrecht. München, C.H. Beck, 646–671.

Johannes, Paul C. und Philipp Richter (2017): Privilegierte Verarbeitung im BDSG-E, Regeln für Archivierung, Forschung und Statistik. Datenschutz und Datensicherheit 41(5), 300–305.

Kipker, Dennis-Kenji und Maren Pollmann (2019): Sozialdatenschutz. In: Louisa Specht und Reto Mantz (Hrsg.): Handbuch Europäisches und deutsches Datenschutzrecht. München, C.H. Beck, 718–761.

LDA Brandenburg [Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht] (2018): Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO. https://www.lda.brandenburg.de/media_fast/4055/DSFA_Muss_Liste_Allgemein_17102018.pdf (Zugriff am 21.12.2019).

RatSWD [Rat für Sozial- und Wirtschaftsdaten] (2017): Forschungsethische Grundsätze und Prüfverfahren in den Sozial- und Wirtschaftswissenschaften. RatSWD Output 9(5). Berlin, Rat für Sozial- und Wirtschaftsdaten (RatSWD). https://doi.org/10.17620/02671.1 (Zugriff am 21.12.2019).

RatSWD [Rat für Sozial- und Wirtschaftsdaten] (2018): Forschungsdatenmanagement in den Sozial-, Verhaltens- und Wirtschaftswissenschaften – Orientierungshilfen für die Beantragung und Begutachtung datengenerierender und datennutzender Forschungsprojekte. RatSWD Output 3(5). Berlin, Rat für Sozial- und Wirtschaftsdaten (RatSWD). https://doi.org/10.17620/02671.7 (Zugriff am 21.12.2019).

RatSWD [Rat für Sozial- und Wirtschaftsdaten] (2019): Tätigkeitsbericht 2018 der vom RatSWD akkreditierten Forschungsdatenzentren (FDZ). Berlin, Rat für Sozial- und Wirtschaftsdaten (RatSWD). https://doi.org/10.17620/02671.40 (Zugriff am 21.12.2019).

ULD [Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein] (2019): Datenschutzbeauftragte. Praxis-Reihe: Datenschutzbestimmungen praktisch umsetzen 2. https://www.datenschutzzentrum.de/praxisreihe (Zugriff am 21.12.2019).

ULD [Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein] (2019a): Informationspflichten. Praxis-Reihe: Datenschutzbestimmungen praktisch umsetzen 4. https://www.datenschutzzentrum.de/praxisreihe (Zugriff am 21.12.2019).

Von Lewinski, Kai (2017): Melderegisterdaten als Grundlage für empirische Sozialstudien. Verwaltungsrundschau 63(1), 1–7.

Winter, Christian; Verena Battis und Oren Halvani (2019): Herausforderungen für die Anonymisierung von Daten. Technische Defizite, konzeptuelle Lücken und rechtliche Fragen bei der Anonymisierung von Daten. Zeitschrift für Datenschutz 9(11), 489–493.

Anhang

Übersicht über die Rechtsgrundlagen der Datenbereitstellung in den akkreditierten Forschungsdatenzentren (FDZ)

Datenzentrum	DSGVO	BDSG	LDSG	SGB	BStatG	KWG	UrhG	Sonstige
Allgemeine Bevölkerungsumfrage der Sozialwissenschaften (ALLBUS)	x	x						
Archiv für Gesprochenes Deutsch (AGD)	x							
Betriebs- und Organisationsdaten (BO)	x	x	x				x	
Beziehungs- und Familienpanel pairfam	x							
Bundesanstalt für Arbeit (BA) im Institut für Arbeitsmarkt und Berufssforschung (IAB)	x			x				
Bundesbank	x				x	x		x[a]
Bundesinstitut für Berufsbildung (BIBB)	x	x		x				x[b]
Bundeszentrale für gesundheitliche Aufklärung (BZgA)	x	x						
Deutsche Rentenversicherung Bund	x			x				
Deutsches Institut für Internationale Pädagogische Forschung (DIPF)	x	x	x				x	
Deutsches Jugendinstitut (DJI)	x							x[c]
Deutsches Zentrum für Altersfragen (DZA)	x	x						
Deutsches Zentrum für Hochschul- und Wissenschaftsforschung (DZHW)	x	x						
Deutsches Zentrum für Integrations- und Migrationsforschung (DeZIM)	x							
eLabour	x	x						
Forschungsinstitut zur Zukunft der Arbeit (IZA)	x							
German Microdata Lab (GML)					x			
German Pharmacoepidemiological Research Database (GePaRD)				x				
ifo Institut – Leibniz-Institut für Wirtschaftsforschung	x	x	x					
Institut zur Qualitätsentwicklung im Bildungswesen (IQB)	x	x						
Internationale Umfrageprogramme	x	x						

Datenzentrum	DSGVO	BDSG	LDSG	SGB	BStatG	KWG	UrhG	Sonstige
Kraftfahrt-Bundesamt (KBA)					x			
Leibniz-Institut für Bildungsverläufe (LIfBi)	x	x						
Leibniz-Institut für Finanzmarktforschung SAFE	x	x	x					
Leibniz-Institut für ökologische Raumentwicklung (IÖR) Monitor		x						x[d]
Leibniz-Institut für Wirtschaftsforschung Halle (IWH)	x	x			x			
Leibniz-Zentrum für Psychologische Information und Dokumentation (ZPID)	x	x	x					
Programme for the International Assessment of Adult Competencies (PIAAC)	x	x						
Qualiservice	x	x	x				x	
Robert Koch-Institut (RKI)	x	x						
RWI – Leibniz-Institut für Wirtschaftsforschung	x	x		x	x			
Sozio-oekonomisches Panel (SOEP)	x							
Statistische Ämter der Länder					x			
Statistisches Bundesamt (destatis)	x				x			x[e]
Stifterverband	x	x			x			
Survey of Health, Ageing and Retirement in Europe (SHARE)	x	x						
Wahlen	x							
Zentrum für Europäische Wirtschaftsforschung (ZEW)	x	x			x			

Hinweis: Stand Mai 2020.
DSGVO = EU-Datenschutzgrundverordnung, BDSG = Bundesdatenschutzgesetz, LDSG = Landesdatenschutzgesetz, SGB = Sozialgesetzbuch, BStatG = Bundesstatistikgesetz, KWG = Kreditwesengesetz, UrhG = Urheberrechtsgesetz.

a EU-Statistikverordnungen, Außenwirtschaftsgesetz, privatrechtliche Verträge mit Geschäftspartnern
b § 90 Berufsbildungsgesetz (BBIG)
c Bundeshaushaltsordnung (BHO): Zuwendungsbescheid
d Geodatenzugangsgesetz (GeoZG)
e EU VO Nr. 557/2013

Mitwirkende

bei der Überarbeitung für die 2. Auflage

Überarbeitung

Prof. Dr. Matthias Bäcker
Johannes Gutenberg-Universität Mainz

Dr. Sebastian Golla
Johannes Gutenberg-Universität Mainz

Konsultationsgruppe des RatSWD

Prof. Dr. Cordula Artelt
Leibniz-Institut für Bildungsverläufe (LIfBi)

Prof. Stefan Bender
Deutsche Bundesbank

Dr. Jan Goebel
Sozio-oekonomisches Panel (SOEP) am DIW Berlin

Heike Habla
Statistisches Bundesamt

Eckart Hohmann

Dr. Cornelia Lange
Robert Koch-Institut (RKI)

Bertram Raum
Datenschutzexperte

Prof. Regina T. Riphahn, Ph.D.
Friedrich-Alexander-Universität Erlangen-Nürnberg

Dr. Heike Wirth
GESIS – Leibniz-Institut für Sozialwissenschaften

Geschäftsstelle des RatSWD

Dr. Mathias Bug

Thomas Runge

Mitwirkende bei der Erstellung der 1. Auflage

Autorinnen und Autoren

Tobias Gebel
Deutsches Institut für Wirtschaftsforschung (DIW Berlin)

Heike Habla
Statistisches Bundesamt

Dr. Cornelia Lange
Robert Koch-Institut (RKI)

Alexia Meyermann
DIPF | Leibniz-Institut für Bildungsforschung und Bildungsinformation

Prof. Regina T. Riphahn, Ph.D.
Friedrich-Alexander-Universität Erlangen-Nürnberg

Daniel Schmidutz
Max-Planck-Institut für Sozialrecht und Sozialpolitik (MPISOC)

Geschäftsstelle des RatSWD

Claudia Oellers

Thomas Runge

Impressum

Herausgeber:
Rat für Sozial- und Wirtschaftsdaten (RatSWD)
Rungestr. 9
10179 Berlin
office@ratswd.de
https://www.ratswd.de

Redaktion:
Thomas Runge, Dr. Mathias Bug, Dr. Katrin Schaar

Gestaltung/Satz:
Claudia Kreutz

Icons:
made by Freepik from www.flaticon.com
Font Awesome, fontawesome.com (angepasst)

Berlin, Juni 2020

RatSWD Output:
Die RatSWD Output Series dokumentiert die Arbeit des RatSWD in seiner 6. Berufungsperiode (2017–2020). 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 (BMBF) unter dem Förderkennzeichen 01UW1802 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt, sofern nicht anders ausgewiesen, beim RatSWD.

doi: 10.17620/02671.50

Zitationsvorschlag:
RatSWD [Rat für Sozial- und Wirtschaftsdaten] (2020): Handreichung Datenschutz. 2. vollständig überarbeitete Auflage. RatSWD Output 8 (6). Berlin, Rat für Sozial- und Wirtschaftsdaten (RatSWD). https://doi.org/10.17620/02671.50.

Der Rat für Sozial- und Wirtschaftsdaten (RatSWD) berät seit 2004 die Bundesregierung und die Regierungen der Länder in Fragen der Forschungsdateninfrastruktur für die empirischen Sozial-, Verhaltens- und Wirtschaftswissenschaften. Im RatSWD arbeiten acht durch Wahl legitimierte Vertreterinnen und Vertreter der sozial-, verhaltens- und wirtschaftswissenschaftlichen Fachdisziplinen mit acht Vertreterinnen und Vertretern der wichtigsten Datenproduzenten zusammen.

Er versteht sich als institutionalisiertes Forum des Dialoges zwischen Wissenschaft und Datenproduzenten und erarbeitet Empfehlungen und Stellungnahmen. Der RatSWD engagiert sich für eine Infrastruktur, die der Wissenschaft einen breiten, flexiblen und sicheren Datenzugang ermöglicht. Solche Daten werden von staatlichen, wissenschaftsgetragenen und privatwirtschaftlichen Akteuren bereitgestellt. Der RatSWD hat 38 Forschungsdatenzentren (Stand: Mai 2020) akkreditiert, deren Kooperationen er fördert.

www.ratswd.de