DiP-iT
Digitales Programmieren im Team

Stand: November 2022

Maßnahmenkatalog zu Datenschutz und Forschungsdatenmanagement

Ian Wolff (Otto-von-Guericke-Universität Magdeburg)
https://orcid.org/0000-0002-0413-0035

Videoserie: Zum Datenschutz im Zusammenhang mit dem Forschungsdatenmanagement wird die Videoserie von Ziedorn und Soßna „Umgang mit personenbezogenen Forschungsdaten“ empfohlen.

Inhalt

Finanzierung: Diese Arbeit wurde im Rahmen des Projektes DiP-iT in der Förderlinie zur Digitalen Hochschulbildung vom deutschen Bundesministerium für Bildung und Forschung unterstützt [Förderkennzeichen 16DHB 3007 und 16DHB 3008].

1. Rechtlicher Rahmen des Datenschutzes

1.1 Datenschutzgrundverordnung (DSGVO)

Die DSGVO findet Anwendung, wenn

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

Definition personenbezogene Daten und besondere Kategorien

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. (RatSWD 2020, S. 9)

Beispiele personenbezogener Daten:

- Name von Probanden
- E-Mail-Adresse
- Anschrift oder Telefonnummer
- Genetische oder biometrische Daten
- Gesundheitsdaten
- Matrikelnummer von Studierenden
- Usernamen auf Onlineplattformen oder andere Online-Kennungen (forschungsdaten.info)

Für besonderer Arten personenbezogener Daten ist ein zusätzlicher Schutz vorgesehen. Zu dieser Art von Daten zählen (Art. 9 Abs. 1 DSGVO):

- rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung

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. (RatSWD 2020, S. 10)

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, ebenso der Nachvollziehbarkeit wie die Pflichten zur proaktiven Information des Betroffenen. Auch das Auskunftsrecht (Art. 15 DSGVO) dient der Transparenz. (RatSWD 2020, S. 11)

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. (RatSWD 2020, S. 11)

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). (RatSWD 2020, S.12)

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. (RatSWD 2020, S. 13)

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 Vorgaben. (RatSWD 2020, S. 13)

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*." (RatSWD 2020, S. 13)

2. Maßnahmen zum Datenschutz im Forschungsdatenlebenszyklus

2.1 Design- und Erhebungsphase

Datensparsamkeit

Weiterhin gilt der Grundsatz der Erforderlichkeit sowie das Prinzip der Datenvermeidung und -sparsamkeit, d. h. es sind *„so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen*". In der Regel sind persönliche Daten, sobald es der Forschungszweck erlaubt, zu anonymisieren. (forschungsdaten.info)

1. Maßnahmen - Fragen zur Datensparsamkeit -

- Müssen personenbezogene Daten erhoben werden?
- Sind die Daten denn wirklich relevant zum Erreichen der Projektziele?
- Wann können sie gelöscht oder anonymisiert/pseudonymisiert werden, ohne das Erreichen des Projektziels zu gefährden?
- Müssen Studienteilnehmer/innen unter Umständen zu einem späteren Zeitpunkt erneut kontaktiert werden (nächste Welle in einer Panelstudie, Nachfolgeprojekt etc.)? (Watteler S.75)

Merke: Eine Nachnutzung von Daten erfüllt auch das datenschutzrechtliche Gebot der Datenminimierung: *„Personenbezogene Daten müssen […] c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“* (Art. 5 Abs. 1c DSGVO). D.h., Forscher/innen erheben keine eigenen Daten und damit werden zu beforschende Personen weniger oft auf eine Teilnahme angesprochen. Da für die genannten Daten bereits Regelungen getroffen wurden, konzentrieren wir uns im Folgenden auf die Erhebung eigener Daten. (Watteler, S. 62)

Einwilligung

Das Vorgehen beim Umgang mit Daten im Forschungsvorhaben und im Anschluss ist Teil der informierten Einwilligung. Die datenschutzrechtlichen Vorgaben zu Einwilligungen umfassen, die **Informiertheit**, die **Zweckbindung** und die **Freiwilligkeit**. Befragte müssen vollständig über die Verwendung ihrer Daten aufgeklärt werden, damit sie wirksam einwilligen können. (Watteler, S. 62)

Die Einwilligung muss informiert erfolgen (informed consent), d.h., der Einwilligende muss durch entsprechende Vorabinformationen seitens der datenerhebenden Wissenschaftler genau nachvollziehen können, welche seiner persönlichen Daten **wie, für was, von wem und wie lange** verwendet werden sollen. Hierzu ist es erforderlich, dass die Informationen in **präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache** an den Betroffenen übermittelt werden (Art. 7 Abs. 2 S. 1 und Art. 12 Abs. 1 S. 1 DSGVO) und die betroffene Person vor allem über die **Verantwortlichen**, den **Verarbeitungszweck**, die **Freiwilligkeit**, die **Folgen**, die **Speicherdauer**, mögliche sonstige **Datenempfänger** im In- und Ausland, den zuständigen **Datenschutzbeauftragten** und die **Aufsichtsbehörde** sowie die bestehenden **Betroffenenrechte** informiert wird (vgl. Art. 13 und 14 DSGVO). Die betroffene Person soll also in die Lage versetzt werden, die Konsequenzen der eigenen Einwilligung genau einschätzen zu können. (Baumann, S. 15)

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 eingeschränkt, wohl aber die Notwendigkeit, die Einwilligung nur auf einen oder mehrere konkret festgelegte Zwecke zu beschränken. (RatSWD 2020, S. 21) Weit gefassten Einwilligungserklärungen (z. B. *„Ich willige ein, dass meine personenbezogenen Daten über den Rahmen der beschriebenen Studie hinaus auch Dritten für derzeit noch unbekannte Vorhaben zu Zwecken der Bildungsforschung weitergegeben werden können“*) ist als Korrektiv das Recht der Einwilligenden zur Seite gestellt, ihre Einwilligung (mit Wirkung für die Zukunft) jederzeit ohne Angabe von Gründen widerrufen zu können. (RatSWD 2017, S. 25)

Erhebung **besonderer personenbezogener Daten** erfordert eine spezifische Einwilligungserklärung.

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). (Rat SWD 2020, S. 17)

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

Es muss ein **Zweck wissenschaftlicher Forschung** vorliegen. Dafür ist ein konkretes Forschungsvorhaben notwendig, das dem Aufbau und Inhalt nach wissenschaftlichen Ansprüchen genügt. 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. (Rat SWD 2020, S. 18)

2. Maßnahmen - Einwilligungserklärung -

- Die Teilnehmende darüber informieren, wie Forschungsdaten gespeichert, erhalten und langfristig verwendet werden sollen.
- Teilnehmende darüber informieren, wie die Vertraulichkeit eingehalten wird, z.B. durch eine Anonymisierung der Daten.
- Teilnehmende über Widerrufsrecht und Recht auf Löschung informieren. (Opt-Out)
- Eine schriftliche Zustimmung für die Datenübertragung, Datenverarbeitung und Datenarchivierung einholen. (forschungsdaten.info)

2.2 Aufbereitungs- und Analyse

Pseudonymisierung

Die DSGVO Pseudonymisierung in Art. 4 Abs. 5 als eine „*Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können*". Diese wird durch Datentrennung erreicht. Dazu werden identifizierende von sonstigen Angaben getrennt und in einem zweiten Datensatz untergebracht. Beide Datensätze sind durch eindeutige Zuordnungsschlüssel (Pseudonyme) wieder miteinander verknüpfbar. Die Möglichkeit der Feststellung der wahren Identität bleibt erhalten.

Neben der Pseudonymisierung sollten personelle und technische Maßnahmen genutzt werden, die eine unkontrollierte Verbreitung von Dateien mit sensiblen Inhalten verhindern. Dazu zählt, die Verarbeitung der Daten auf bestimmte Personen zu beschränken. Nur Bearbeiter/innen, die mit den Bestimmungen des Datenschutzes vertraut ist, sollten im Projekt über Zugriffsrechte auf die (in der Regel mindestens pseudonymisierten) Daten verfügen. Die Daten sollten zudem nicht ungeschützt auf Netzlaufwerken abgelegt werden. In aller Regel gelangen Daten auf Netzlaufwerken nämlich (automatisiert) in Backups des Instituts oder eines Rechenzentrums. Zur Sicherung der personenbezogenen Merkmale bieten sich hier verschiedene Formen der technischen Verschlüsselung an. (Watteler, S. 64)

Anonymisierung

Anonymisierung bedeutet die Tilgung des Personenbezugs von Daten. **Sind Daten anonymisiert, ist die DSGVO auf ihre Verarbeitung nicht mehr anwendbar.** Anders als die alte Fassung des BDSG enthält die DSGVO keine Definition des Begriffs Anonymisieren. 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.

Faktische Anonymisierung entspricht der Teildefinition des bisherigen alten BDSG (§ 3 Abs. 6) zu Anonymisierung, nach der Einzelangaben *„nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können*".

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 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, 658f). Ein besonderes Gebot der Anonymisierung enthält auch § 27 Abs. 3 Satz 1 BDSG für besondere Kategorien personenbezogener Daten, die zu Forschungszwecken verarbeitet werden.

3. Maßnahme - Pseudonymisierung und Anonymisierung -

- Pseudonymisierung personenbezogener Daten mittels geeigneter technischer Rahmenbedingungen
  - Verarbeitung der Daten auf bestimmt Personen beschränken
  - Daten nur geschützt auf Netzwerklaufwerken hinterlegen
  - Zur Sicherung der personenbezogenen Merkmale bieten sich verschiedene Formen der technischen Verschlüsselung an
- Bei Anonymisierung sollte faktisch anonymisiert werden

2.3 Veröffentlichungs- oder Archivierungsphase

Durch die Nutzung von Datenzentren oder auch Archiven ist es möglich, den Zugriff auf vertrauliche und sensible Daten zu beschränken und zugleich eine Datenfreigabe für Forschungs- und Bildungszwecke zu ermöglichen. Die in Datenzentren und Archiven gehaltenen Daten sind im Allgemeinen nicht öffentlich zugänglich. Ihre Verwendung nach der Benutzerregistrierung ist auf bestimmte Zwecke beschränkt. Nutzerinnen und Nutzer unterzeichnen eine Endbenutzer-Lizenz, in der sie sich mit bestimmten Bedingungen einverstanden erklären, z. B. Daten nicht zu kommerziellen Zwecken zu nutzen oder potenziell identifizierbare Personen nicht zu identifizieren. Welche Art von Datenzugriff erlaubt ist, wird vorher mit der Urheberin und dem Urheber festgelegt. (forschungsdaten.info)

Datenzentren können zusätzliche Zugangsregelungen für vertrauliche Daten verhängen. Dazu zählen:

- Notwendigkeit einer speziellen Genehmigung vom Urheber für den Zugang zu den Daten
- Belegung vertraulicher Daten mit einem Embargo für einen bestimmten Zeitraum
- Bereitstellung des Zugangs nur für zugelassene Forscher
- Bereitstellung von sicherem Datenzugriff, in dem eine Fernanalyse von vertraulichen Daten durchgeführt werden kann, jedoch die Daten nicht herunterladen werden können
- Entscheidung über eine Veröffentlichung als PUF oder SUF (forschungsdaten.info)

Public Use File: Daten in Public Use Files (PUF) sind normalerweise so weit anonymisiert, dass sie zu öffentlichen Zwecken zugänglich sind

Scientific Use File: Daten in Scientific Use Files (SUF) sind so weit anonymisiert, dass sie zu Forschungszwecken verwendet werden dürfen. Sie bieten im Vergleich zu den On-Site-Zugangswegen ein geringeres Analysepotential, sind jedoch so konzipiert, dass sie sich für einen großen Teil der wissenschaftlichen Forschungsvorhaben eignen. (Watteler S. 72)

4. Maßnahme - Vorkehrungen zur Datenpublikation und Archivierung – (RatSWD 2016, S. 17)

- Prüfen, ob Daten vorliegen, die gelöscht werden müssen
  - Hier sind insbesondere die Vorgaben zur Datenarchivierung durch den beispielsweise Drittmittelförderer, Universitäten oder Forschungsinstitute zu beachten.
- Zur Verfügung stellen der Daten zur Nachnutzung
  - Zugänglichkeit der Daten (Repositorium, Forschungsdatenzentrum)
  - Zugangswege der Daten für eine Sekundäranalyse (SUF, PUF)
  - Zeitpunkt der Datenveröffentlichung
  - Dauerhafte Auffindbarkeit der Daten garantieren durch einen persistenten Identifikator (bspw. DOI)
  - Datenformate
  - Dokumentation der Daten
- Beschränkungen zur Datennachnutzung
  - Bedingungen und Restriktionen zur Nachnutzung der Daten, die sich aus deren Eigenschaften ableiten (bspw. personenbezogenen Daten)

Eine spezielle Regelung für die **Veröffentlichung besonderer Kategorien personenbezogener Daten** zu Forschungszwecken trifft § 27 Abs. 4 BDSG. Voraussetzung für eine Veröffentlichung ist demnach, dass die betroffene Person eingewilligt hat 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.

Literaturverzeichnis

Baumann, Paul; Lauber-Rönsberg, Anne; Krahn, Philipp: Gutachten zu den rechtlichen Rahmenbedingungen des Forschungsdatenmanagements, Kurzfassung. Dresden 2018. Online: <https://tu-dresden.de/gsw/phil/irget/jfbimd13/ressourcen/dateien/dateien/DataJus/DataJus_Zusammenfassung_Gutachten_12-07-18.pdf?lang=de>, Stand: 20.10.2022.

Datenschutzrecht, **forschungsdaten.info**, 24.09.2021, <https://forschungsdaten.info/themen/rechte-und-pflichten/datenschutzrecht/#c279470>, Stand: 20.10.2022.

Gola, Peter: Datenschutz-Grundverordnung VO (EU) 2016/679. Kommentar, München 2017.

Kapitel 6 – datenschutzrechtliche Rahmenbedingungen, in: **Baumann, Paul; Krahn, Philipp; Lauber-Rönsberg, Anne**, Forschungsdatenmanagement und Recht. Datenschutz-, Urheber- und Vertragsrecht, Feldkirch/Düns 2021, S. 165-277.

Lipp, Silvia: Learning Analytics – Datenschutzrechtliche Bestimmungen als Ausgangspunkt einer verantwortungsvollen Nutzung von Bildungsdaten, in: Bachor, Martina; Hug, Theo; Pallaver, Günther (Hg.), DataPolitics. Zum Umgang mit Daten im digitalen Zeitalter, Innsbruck 2021, S. 121-134. Online: <https://library.oapen.org/bitstream/id/a3d38ad0-bbc9-4a7b-9881-1f6b1de66c7d/9783991060468.pdf>, Stand: 20.10.2022.

RatSWD – Rat für Sozial- und Wirtschaftsdaten: Handreichung Datenschutz. 2. vollständig überarbeitete Auflage. RatSWD Output 8(6), Berlin 2020. Online: <https://doi.org/10.17620/02671.50>, Stand: 20.10.2022.

RatSWD – Rat für Sozial- und Wirtschaftsdaten: Handreichung Datenschutz. Output Series 5, Berlin 2017. Online: <https://www.ratswd.de/dl/RatSWD_Output5_HandreichungDatenschutz.pdf>, Stand 20.10.2022.

RatSWD – Rat für Sozial- und Wirtschaftsdaten (2016): Forschungsdatenmanagement in den Sozial-, Verhaltens- und Wirtschaftswissenschaften. Orientierungshilfen für die Beantragung und Begutachtung datengenerierender und datennutzender Forschungsprojekte, Output Series 3, Berlin 2016. Online: <http://www.ratswd.de/dl/RatSWD_Output3_Forschungsdatenmanagement.pdf>, Stand: 20.10.2022.

Watteler, Oliver; Ebel, Thomas: Datenschutz im Forschungsdatenmanagement, in: Jensen, Uwe; Netscher, Sebastian; Weller, Katrin (Hg.), Forschungsdatenmanagement sozialwissenschaftlicher Umfragedaten. Grundlagen und praktische Lösungen für den Umgang mit quantitativen Umfragedaten, Opladen u.a. 2019, S. 57-80. Online: <https://doi.org/10.3224/84742233>, Stand: 20.10.2022.