vogel—partner
RECHTSANWÄLTE

Datenschutz und Persönlichkeitsrechte in der Bürgerforschung

Rechtliches Kurzgutachten für das Museum für Naturkunde, Berlin

Dr. Uwe K. Schneider

Stand: 21.12.2020

Autor:

Dr. iur. Uwe K. Schneider

Vogel & Partner Rechtsanwälte mbB, Emmy-Noether-Straße 17, 76131 Karlsruhe

Stand: 21.12.2020, Version 1.1

Der Autor dankt Herrn Rechtsreferendar Christian Blaicher für seine Unterstützung bei der Anfertigung dieses Gutachtens, insbesondere bei der Erstellung der Abbildungen.

Gutachten zum Projekt „Rechtliche Rahmenbedingungen der Bürgerforschung" im Auftrag des

Museums für Naturkunde Berlin

Leibniz-Institut für Evolutions- und Biodiversitätsforschung

Gefördert durch das Bundesministerium für Bildung und Forschung

Online dauerhaft auffindbar und zitierbar über:

https://doi.org/10.7479/akea-zg02

Inhaltsverzeichnis

I. Was ist Bürgerforschung bzw. Citizen Science?

Bei der Bürgerwissenschaft (englisch: Citizen Science) handelt es sich um eine freie Form der offenen Wissenschaft, bei der wissenschaftliche Erkenntnisse von Personen gewonnen oder vermittelt werden, die nicht hauptberuflich in der fachzugehörigen Wissenschaft tätig sind. Bei der Beteiligung an der Gewinnung von Erkenntnissen durch entsprechende Personen spricht man auch von Bürgerforschung. Die Beteiligung kann verschiedene Phasen des Forschungsprozesses umfassen und kann von der Schaffung von Fragestellungen, der Entwicklung von Forschungsprojekten über die Datenerhebung und Datenverarbeitung bis hin zur Veröffentlichung der Forschungsergebnisse reichen. Das Bundesministerium für Bildung und Forschung (BMBF) unterstützt und fördert seit 2013 die Bürgerwissenschaften, u. a. den Dialogprozess des Bausteinprogramms BürGEr schaffen WISSen – Wissenschafft Bürger (GEWISS)[1], um grundlegende Fragen der Bürgerforschung zu diskutieren.[2] Das hierdurch geschaffene Grünbuch definiert Citizen Science als

> „**Beteiligung von Personen an wissenschaftlichen Prozessen, die nicht in diesem Wissenschaftsbereich institutionell gebunden** sind. Dabei kann die Beteiligung in der kurzzeitigen Erhebung von Daten bis hin zu einem intensiven Einsatz von Freizeit bestehen, um sich gemeinsam mit Wissenschaftlerinnen bzw. Wissenschaftlern und/oder anderen Ehrenamtlichen in ein Forschungsthema zu vertiefen. Obwohl viele ehrenamtliche Forscherinnen und Forscher eine akademische Ausbildung aufweisen, ist dies keine Voraussetzung für die Teilnahme an Forschungsprojekten. Wichtig ist allerdings die Einhaltung wissenschaftlicher Standards, wozu vor allem Transparenz im Hinblick auf die Methodik der Datenerhebung und die öffentliche Diskussion der Ergebnisse gehören".[3]

Citizen Science wird sowohl von der institutionellen Wissenschaft als auch von Behörden initiiert oder in Schulen praktiziert.[4] Nicht entscheidend ist demnach, ob die bürgerliche Forschungstätigkeit auf eigeninitiativer Basis stattfindet (z. B. durch ehrenamtliche Forschungsgruppen) oder durch wissenschaftliche Institutionen initiiert wird (z. B. von Hochschulen, Universitäten oder Museen). Neben GEWISS als zentrale Platzform für Citizen Science und anderen Citizen Science Projekten in Deutschland[5] haben sich mit der European Citizen Science Association (ECSA)[6] über 17 EU-Länder zur Förderung von Citizen Science zusammengeschlossen.

II. Was schützt der Datenschutz?

Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht in der Europäischen Union (EU). So steht es schon im ersten Erwägungsgrund zur Datenschutzgrundverordnung (DSGVO),[7] wo unter anderem das Recht auf Schutz personenbezogener Daten nach der Grundrechtecharta der EU in Bezug genommen wird. Daneben hat in Deutschland das

---

[1] Siehe hierzu die Webseite der GEWISS unter https://www.buergerschaffenwissen.de/.
[2] https://www.bmbf.de/de/citizen-science-wissenschaft-erreicht-die-mitte-der-gesellschaft-225.html.
[3] Grünbuch Citizen Science Strategie 2020 für Deutschland, S. 13. Hier abrufbar: https://www.buergerschaffenwissen.de/sites/default/files/grid/2017/11/20/gewiss-gruenbuch_citizen_science_strategie.pdf
[4] https://www.buergerschaffenwissen.de/citizen-science/handbuch/was-ist-citizen-science.
[5] Einen guten Überblick über die Projektvielfalt bietet: http://www.buergerschaffenwissen.de/:
[6] Siehe hierzu die Webseite der ECSA unter https://ecsa.citizen-science.net/.
[7] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679.

Bundesverfassungsgericht bereits 1983 im sogenannten Volkszählungsurteil ein **Grundrecht** auf informationelle Selbstbestimmung aus dem allgemeinen Persönlichkeitsrecht des Grundgesetzes abgeleitet. Demnach soll grundsätzlich jede und jeder selbst entscheiden können, wem wann welche die eigene Person betreffende Daten zugänglich gemacht und für welche Zwecke diese verarbeitet werden.[8]

Hier wird deutlich, dass es nicht um den Schutz von Daten um ihrer selbst willen geht, sondern um den **Schutz „natürlicher Personen"**, also von Menschen, über welche diese Daten etwas aussagen. Diese Personen, seien es Bürgerforscher/innen[9] oder Dritte, sollen vor einem Missbrauch ihrer Daten geschützt werden.

Das spricht bereits **gegen eine schrankenlose Beobachtung**. Denn wer nicht mehr wissen kann, wer was wann und bei welcher Gelegenheit über ihn weiß, wird versucht sein, nicht aufzufallen. Dies beeinträchtigt, so das Bundesverfassungsgericht, nicht nur individuelle Entfaltungschancen des Einzelnen, sondern auch das freiheitlich demokratische Gemeinwesen, welches der selbstbestimmten Mitwirkung seiner Bürger bedarf.

Daraus folgen auch **Grenzen im Bereich Citizen Science**, so für dort tätige Institutionen, was eine Erfassung des Verhaltens der Bürgerforscher oder Dritter angeht, ebenso aber für die Bürgerforscher selbst, wenn sie Daten Dritter erfassen. Vor diesem Hintergrund kann z. B. auch die namentliche Nennung der Bürgerforscher gerade in der Öffentlichkeitsarbeit zu Zurückhaltung beim Beitragen von Beobachtungen und Bewertungen führen, es sei denn, ein Bürgerforscher wünscht diese Nennung ausdrücklich als Anerkennung.

Neben der **Vertraulichkeit** von persönlichen Informationen, als eine Voraussetzung der freien Entfaltung der Persönlichkeit, will der Datenschutz unter anderem aber auch die **Verfügbarkeit**, Unverfälschtheit (**Integrität**) und die sachliche **Richtigkeit** von personenbezogenen Daten gewährleisten. Dies deckt sich insoweit mit den allgemeinen Anforderungen an ein Forschungsdatenmanagement. So soll vermieden werden, dass aus falschen oder unvollständigen Daten ein Zerrbild über eine Person entsteht. Die vollständige Erfassung einer Person kann aus den bereits genannten Gründen in der Regel – zumindest ohne deren Einwilligung – jedoch keine Lösung dieses Dilemmas sein, sondern ein sorgfältiger Umgang mit den Daten in dem Bewusstsein, dass sie eine Person nie vollständig abbilden.

Zum Beispiel ist es zwar auch für die Bürgerforschung ein legitimes Ziel Umweltverschmutzung zu ergründen. Wenn hierfür identifizierbare Personen beim Abladen von Müll beobachtet werden und dies dokumentiert wird, ist jedoch Vorsicht geboten. Möglicherweise muss der Personenbezug entfernt werden. Jedenfalls dürfen diese Personen nicht wegen eines singulären Aktes an den Pranger gestellt und diese Daten in identifizierbarer Form veröffentlicht werden. Sonst könnten unangemessene Benachteiligungen dieser Personen drohen.

Der Schutz setzt jedoch bereits an der bloßen **Verarbeitung personenbezogener Daten** und damit im **Vorfeld konkreter Beeinträchtigungen** einer Person an, da letztere präventiv verhindert werden sollen. Dementsprechend unterliegt eine solche Verarbeitung einem Verbot mit Erlaubnisvorbehalt. Das bedeutet, dass die Verarbeitung nur mit Einwilligung der betroffenen Person oder auf Grundlage einer

[8] Im Folgenden wird der einfacheren Sprache halber in der Regel jeweils nur die männliche Form verwendet, welche jedoch immer auch die weibliche Form oder andere Geschlechtsidentitäten einschließt.
[9] Auch insoweit wird der einfacheren Sprache halber in der Regel einheitlich der Begriff „Bürgerforscher" verwendet. Die grammatikalisch männliche Form meint jedoch immer auch die weibliche Form oder andere Geschlechtsidentitäten.

gesetzlichen Erlaubnis zulässig ist. Dieses Erfordernis einer Rechtsgrundlage für jede Datenverarbeitung wird in der DSGVO über den Grundsatz der Rechtmäßigkeit adressiert. Daneben gibt es weitere Grundsätze wie den der Zweckbindung oder der Speicherbegrenzung, die ebenfalls einzuhalten sind.

Zwar enthält die DSGVO für die Datenverarbeitung zu **Zwecken der wissenschaftlichen und historischen Forschung** gewisse Privilegierungen. Eine Komplettausnahme vom Datenschutz besteht für die Forschung, auch die Bürgerforschung, jedoch keineswegs. Um Sanktionen und Imageverlust zu vermeiden sowie den berechtigten Interessen der betroffenen Personen gerecht zu werden, sind daher die jeweils geltenden Regelungen sorgfältig einzuhalten. Dieses Kurzgutachten gibt einen Überblick über diese Regelungen.

III. Gilt für die Datenverarbeitung durch Bürgerforscher/innen das Datenschutzrecht überhaupt – und, wenn ja, welches?

1. Die Datenschutz-Grundverordnung der EU (DSGVO)

Seit dem 25.05.2018 ist die DSGVO zu beachten. Sie gilt für die Verarbeitung personenbezogener Daten, soweit diese im Rahmen von Tätigkeiten einer Niederlassung in der EU erfolgt. Hat ein Datenverarbeiter keine Niederlassung in der EU, gilt die DSGVO, wenn die Verarbeitung in Zusammenhang damit steht, dass betroffenen Personen in der EU Leistungen angeboten werden oder ihr Verhalten beobachten wird.

Der entsprechende räumliche **Geltungsbereich** (Art. 3 DSGVO) ist für Institutionen mit Sitz in der EU, welche die Bürgerforschung initiieren oder koordinieren, folglich eröffnet. Dies gilt auch für die Bürgerforscher selbst, soweit diese in der EU ansässig sind oder dort das Verhalten von Menschen beobachten.

Der sachliche Anwendungsbereich der DSGVO ist eröffnet, wenn personenbezogene Daten verarbeitet werden und dies entweder automatisiert oder in einem Dateisystem geschieht (Art. 2 Abs. 1 DSGVO).

> **Verarbeitung** bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten (Art. 4 Nr. 2 DSGVO).

Abbildung 1: Regelbeispiele für Verarbeitungsvorgänge

Der Verarbeitungsbegriff stellt also nicht auf die Automatisierung mittels Informationstechnik bzw. elektronischer Datenverarbeitung ab und erfasst daher zum Beispiel auch ein manuelles, also händisches Umsortieren von Daten auf Papier. Der sachliche Anwendungsbereich der DSGVO setzt jedoch voraus, dass dies entweder (ganz oder teilweise) automatisiert oder in einem oder für ein Dateisystem erfolgt.

Eine **automatisierte Verarbeitung** liegt beim Einsatz von Datenverarbeitungsanlagen vor, in welche Daten eingegeben, dort verarbeitet und wieder ausgegeben werden. Heute handelt es sich dabei typischerweise um elektronische Systeme, historisch kann man zum Beispiel aber auch Lochkartenautomaten dazu zählen. Teilautomatisiert ist die Verarbeitung, wenn manuelle Zwischenschritte enthalten sind, so beispielsweise, wenn Beobachtungen händisch in ein **Tabellenkalkulationsprogramm** oder eine **Smartphone-App** eingetragen werden müssen, bevor sie dort automatisiert weiterverarbeitet werden. Bei der vollständig automatisierten Verarbeitung sind keine manuellen Zwischenschritte von der Erhebung bis zur Ausgabe der Ergebnisse erforderlich, so zum Beispiel, wenn von einer Smartphone-App das Bewegungsprofil einer betroffenen Person automatisch erfasst und an einen Server gesandt würde.

Bei der Verarbeitung von Daten, die in einem **Dateisystem** gespeichert oder hierfür vorgesehen sind, handelt es sich nach der DSGVO um eine manuelle und damit gerade nicht automatisierte Verarbeitung. Unter einem Dateisystem versteht man hier die **Sammlung von personenbezogenen Daten**, die gleichartig aufgebaut und nach bestimmten Merkmalen zugänglich sowie auswertbar sind. Dies muss mangels Automatisierung gerade kein elektronisches Dateisystem sein, sondern kann auch über entsprechende Strukturierungsmerkmale in **Erfassungsbögen, Akten oder Karteikarten auf Papier** erfolgen. Eine Sortierung kann beispielsweise nach Namen oder Forschungsprojekten stattfinden.

Zwar gab es in der Geschichte der **Wissenschaft** auch Zufallsentdeckungen wie die des Penicillins. Diese stellten aber immer nur den Ausgangspunkt für weitere Forschungen dar. Da die Forschung selbst, auch die Bürgerforschung, ein methodisches und **strukturiertes Vorgehen** erfordert,[10] werden Forschungsdaten praktisch immer zumindest in einem Dateisystem im eben beschriebenen Sinne, wenn nicht sogar in der Regel jedenfalls teilweise automatisiert verarbeitet werden. Haben diese Daten einen Personenbezug, ist daher auch der Anwendungsbereich des Datenschutzrechts eröffnet.[11]

2. Die Öffnungsklauseln der DSGVO für Bund und Länder

Zwar hat die DSGVO als europäische Verordnung durch ihre unmittelbare Wirksamkeit gegenüber den nationalen Vorschriften prinzipiell Vorrang. Jedoch sieht sie durch sogenannte Öffnungsklauseln die Möglichkeit vor, dass die EU-Mitgliedstaaten hinsichtlich bestimmter Fragen ergänzende oder einschränkende Regelungen zum Datenschutz treffen können. Die Bundesrepublik Deutschland hat hiervon durch das neue **Bundesdatenschutzgesetz (BDSG)**[12] sowie die einzelnen Bundesländer mit ihren jeweiligen **Landesdatenschutzgesetzen (LDSG)**[13] Gebrauch gemacht. Für die Bürgerforscher als Privatpersonen, die – wenn gegebenenfalls auch initiiert oder koordiniert durch Forschungsinstitutionen, aber

---

[10] Zu den Anforderungen an das Vorliegen wissenschaftlicher Forschung siehe unten S. 18 f.

[11] Am Rande sei erwähnt, dass für die Anwendung auf die Verarbeitung von Beschäftigtendaten nach § 26 Abs. 7 BDSG nicht einmal das Erfordernis eines manuellen Dateisystems gilt und daher auch nur mündliche Fragen, ohne dass die Antworten entsprechend gespeichert werden sollen, dem Datenschutzrecht unterliegen.

[12] Das BDSG ist u. a. hier abrufbar: https://www.gesetze-im-internet.de/bdsg_2018/.

[13] Eine Übersicht mit Verlinkung auf die einzelnen LDSG findet sich u. a. hier: https://www.bvdnet.de/datenschutzgesetze-der-bundeslaender-an-die-ds-gvo-angepasst/.

versehen mit eigenem Beurteilungs- und Entscheidungsspielraum – Forschung betreiben, gilt in der Regel ergänzend zur DSGVO lediglich das BDSG.

3. In der Regel keine Anwendung der Ausnahme für private Haushalte von der DSGVO

Die DSGVO findet jedoch insbesondere dann keine Anwendung, wenn die Datenverarbeitung nach Art. 2 Abs. 2 Buchstabe c DSGVO **ausschließlich im persönlichen oder familiären Bereich** erfolgt. Nach der Rechtsprechung des Europäischen Gerichtshofs (EuGH) ist diese sogenannte Haushaltsausnahme jedoch eng auszulegen. So wurde die Datenerhebung durch Mitglieder der Zeugen Jehovas unter anderem wegen des übergeordneten Missionierungszwecks nicht als ausschließlich persönlich oder familiär angesehen, selbst wenn die Mitglieder die vor allem an der Haustüre von Andersgläubigen erhobenen Daten nicht an eine Zentrale der Gemeinschaft weitergeleitet, sondern nur persönlich verwaltet haben.[14]

Trotz aller Unterschiede zu den Zeugen Jehovas kann man daraus für die **Bürgerforschung** folgern, dass diese jedenfalls dann nicht unter die Haushaltsausnahme fällt, wenn sie einem übergreifenden Forschungszweck dient, insbesondere wenn dieser von einer Forschungseinrichtung initiiert oder koordiniert wird. Dies dürfte unabhängig davon gelten, ob personenbezogene Daten an diese Institution weitergegeben werden oder nicht. Spätestens wenn Daten den persönlichen oder familiären Bereich verlassen, also eine solche Weitergabe, ein Teilen mit anderen Personen außerhalb der eigenen Familie oder gar eine Veröffentlichung erfolgt, worauf Forschung üblicherweise ausgelegt ist, **kann diese Ausnahme jedoch nicht mehr greifen**.

Letztlich verbleibt für die Haushaltsausnahme also nur der enge persönliche Bereich. Hierunter fallen beispielsweise private Fotografien, wie die Anfertigung von Familienfotos und deren Teilen innerhalb der Familie für private Zwecke. Sollen diese privaten Daten allerdings später zum Beispiel für die historische Bürgerforschung verwendet werden, gelten wieder die eben gemachten Ausführungen, die in aller Regel zur Anwendung der DSGVO führen.

IV. Welches Datenschutzrecht gilt für Institutionen, die Bürgerforschung initiieren und/oder koordinieren?

Für Institutionen, welche die Bürgerforschung initiieren und/oder koordinieren gilt grundsätzlich ebenfalls die DSGVO sowie ergänzend das BDSG oder die jeweiligen LDSG. Die **DSGVO gilt für öffentliche und nicht-öffentliche Stellen gleichermaßen**. Sie bezieht Einzelpersonen, Unternehmen, sonstige private Organisationen wie Vereine und Stiftungen aber auch Behörden und andere öffentliche Einrichtungen ein.

Ergänzend gilt für **nicht-öffentliche Stellen** wie private Personen (zum Beispiel die Bürgerforscher) oder private Forschungseinrichtungen in der BRD in der Regel einheitlich das **BDSG**, wobei hier die Spielräume für Abweichungen von der DSGVO geringer sind als im öffentlichen Bereich.

Gerade für öffentliche Stellen beinhaltet die DSGVO dagegen eine größere Zahl von Öffnungsklauseln, bei denen mitgliedstaatliche Regelungen die DSGVO ergänzen und teilweise von dieser abweichen können. Das Recht zur Nutzung dieser Öffnungsklauseln innerhalb der Mitgliedstaaten bestimmt sich nach der innerstaatlichen Verteilung der Gesetzgebungskompetenzen.

---

[14] EuGH, Urteil vom 10.07.2018, Az. C-25/17, http://curia.europa.eu/juris/liste.jsf?language=de&num=C-25/17.

Soweit öffentliche **Einrichtungen des Bundes** als initiierende und/oder koordinierende Instanzen der Bürgerforschung tätig werden, findet innerhalb dieser Öffnungsklauseln das **BDSG** Anwendung.

Tritt jedoch die öffentliche **Einrichtung eines Bundeslandes** in dieser Funktion auf, findet das entsprechende **LDSG** Anwendung. Zu den Einrichtungen eines Bundeslandes gehören auch die Stellen landesunmittelbarer Körperschaften wie Kommunen oder Universitäten.[15] So gilt beispielsweise für das Museum für Naturkunde in Berlin als landesunmittelbare Stiftung des öffentlichen Rechts neben der DSGVO das LDSG Berlin.

Diese LDSG ähneln einander, sind aber aufgrund der genannten Öffnungsklauseln in der DSGVO nicht identisch. Im Rahmen des vorliegenden Kurzgutachtens kann auf diese 16 LDSG nicht im Einzelnen eingegangen werden. Die **Grundsätze der DSGVO** werden jedoch auch von sämtlichen LDSG beachtet. Lediglich die Ausgestaltung im Detail, zum Beispiel bei den einzelnen gesetzlichen Erlaubnissen für die Datenverarbeitung zu Forschungszwecken, ist unterschiedlich.

Letztlich ist damit im ersten Schritt, wegen der ergänzenden Regelungen in BDSG und LDSG, doch eine Unterscheidung zwischen nicht-öffentlichen und öffentlichen Stellen erforderlich. Für diese ist nicht primär die Rechtsform maßgeblich, sondern **Trägerschaft und Funktion einer Einrichtung**. Auch wenn eine Forschungseinrichtung als Stiftung oder (eigetragener) Verein des Privatrechts oder (gemeinnützige) GmbH verfasst ist, gilt sie als öffentliche Stelle, falls sie mehrheitlich dem Staat – sei es dem Bund, einem Land oder einer anderen staatlichen Körperschaft – gehört oder der Staat über privatrechtliche Steuerungsgremien maßgebenden Einfluss auf die Einrichtung hat. Dies gilt jedenfalls dann, wenn man die Forschung als öffentliche Aufgabe außerhalb des üblichen wirtschaftlichen Wettbewerbs einordnet, was man bei angewandter Technologieforschung bezweifeln kann, was bei Bürgerforschung aber in der Regel der Fall ist.

V. Welche grundlegenden Rollen haben die verschiedenen Beteiligten?

Neben der betroffenen Person, die bei der Verarbeitung ihrer Daten geschützt werden soll, kennt die DSGVO insbesondere die Rollen des Verantwortlichen und des Auftragsverarbeiters.

> **Verantwortlicher** (englisch: Controller) ist, wer über die **Zwecke** und die **Mittel** der Verarbeitung personenbezogener Daten **entscheidet**. Verantwortlicher kann dabei jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle sein, die wie ein Verantwortlicher handelt (Art. 4 Nr. 7 DSGVO).

Die Pflichten des Datenschutzrechts treffen vor allem den Verantwortlichen. Er muss dafür Sorge tragen, dass alle Grundsätze der DSGVO, auf die noch eingegangen wird, eingehalten werden.

> **Auftragsverarbeiter** (englisch: Processor) ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten **im Auftrag des Verantwortlichen** verarbeitet (Art. 4 Nr. 8 DSGVO).

Verarbeitung im Auftrag bedeutet in diesem Kontext vor allem nach Weisung des Verantwortlichen. Denn Letzterer entscheidet allein über Zwecke und (wesentliche) Mittel der Verarbeitung. Der

[15] Ausgenommen sind lediglich die wenigen Hochschulen des Bundes für öffentlichen Verwaltung und die Universitäten der Bundeswehr, welche dem Bund zugeordnet sind.

Auftragsverarbeiter ist allenfalls berechtigt über technische Details des Mitteleinsatzes mitzuentscheiden, zum Beispiel dahingehend welche Versionen eines Betriebssystems eingesetzt werden. Er hat also weit weniger Freiheitsgrade als der Verantwortliche. Dementsprechend beschränken sich seine Pflichten auch weitgehend auf die Art. 28 DSGVO genannten Regelungen, die neben der weisungsgemäßen Datenverarbeitung insbesondere die Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 DSGVO durch technische und organisatorische Maßnahmen vorsehen.[16]

Für die von der **DSGVO angestrebte lückenlose Abgrenzung der Verantwortlichkeiten** und Pflichten ist daneben auch die folgende Definition des „Dritten" heranzuziehen, wobei dieser in der Regel letztlich ein weiterer, eigenständiger Verantwortlicher ist:

> **Dritter** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten (Art. 4 Nr. 10 DSGVO).

1. Regelfall: Bürgerforscher als Verantwortliche

Demnach sind die Bürgerforscher Verantwortliche, wenn sie über die Zwecke und Mittel der Verarbeitung personenbezogener Daten von anderen entscheiden. In den meisten Fällen wird man wohl von einer Verantwortlichkeit der Bürgerforscher ausgehen müssen. Denn selbst wenn sie mit der initiierenden und/oder koordinierenden Institution wesentliche Zwecke und Mittel vereinbart haben, bleiben den Bürgerforschern in der Regel auch insoweit noch nennenswerte **Freiheiten als eigenständige Forscher**. Auch handeln die Bürgerforscher nicht als Mitarbeiter einer Forschungsinstitution, sondern vielmehr als Privatpersonen, bei denen die Forschungsarbeit lediglich eine selbständige bzw. ehrenamtliche Nebentätigkeit darstellt. Sie unterliegen in der Regel im Gegensatz zu einem Auftragsverarbeiter nicht den Weisungen der genannten Institutionen und gehören diesen auch nicht wie angestellte Forscher an.

Ebenso ist es meist unvermeidlich, dass den Bürgerforschern im Rahmen ihrer Forschungstätigkeit ein Spielraum bleibt. Forschung lebt von Freiheiten bei der Suche nach neuen Erkenntnissen, die noch nicht feststehen und damit auch nicht vorgegeben werden können. Selbst in Fällen, in denen Bürgerforscher primär zur Datenerfassung „im Feld" eingesetzt werden und weniger oder überhaupt nicht zur Datenauswertung und damit der eigentlichen Erkenntnisgewinnung, bleibt insoweit oft keine andere Wahl. Denn selbst wenn ihnen für die Datenerfassung grundsätzliche Vorgaben gemacht werden, verbleibt die Konkretisierung dieser Vorgaben „im Feld" – zum Beispiel welches „Setting" bei Bildern von Umweltverschmutzungen aufgenommen wird – bei den Bürgerforschern.

2. Ausnahmefall: Bürgerforscher als Auftragsverarbeiter oder Quasi-Mitarbeiter

Nur ausnahmsweise, wenn die Bürgerforscher untergeordnete Tätigkeiten, vor allem in der Datenerhebung, nach klaren und engen Weisungen einer Institution durchführen, könnten sie entweder

- als deren **Auftragsverarbeiter** oder
- wie – mehr oder weniger freie – **Mitarbeiter** dieser Institution als deren Teil und unter ihrer unmittelbaren Verantwortung tätig werden.

---

[16] Zur Datensicherheit siehe unten S. 28 f.

Im Fall der Auftragsverarbeitung wäre ein entsprechender Vertrag nach Art. 28 DSGVO zwischen Institution und Bürgerforscher abzuschließen.[17] Im Fall der Tätigkeit wie ein Mitarbeiter wäre neben der Erteilung klarer Weisungen für die Datenverarbeitung eine Verpflichtung auf den Datenschutz angezeigt.[18]

3. Verantwortung einer initiierenden/koordinierenden Institutionen

Auch Institutionen, welche die Bürgerforschung initiieren und/oder koordinieren, sind in der Regel Verantwortliche. Denn auch sie entscheiden meist mit über Zweck und Mittel der Datenverarbeitung, insbesondere im Fall der **Weiterverarbeitung von Daten**, die vom Bürgerforscher an die Institution übermittelt werden, aber auch, wenn sie im Vorfeld **Einfluss auf die Forschungskonzeption** haben, zum Beispiel durch Festlegung der Kategorien von zu erfassenden Daten.

4. Abgrenzung der Verantwortung von Institution und Bürgerforscher

Fraglich ist daher, inwieweit die Bürgerforscher und die genannten Institutionen füreinander bzw. untereinander verantwortlich sind oder wie man die Verantwortungssphären voneinander abgrenzen kann. Dabei sind folgende Grundkonstellationen denkbar:

- **Auftragsverarbeitung** (Controller-to-Processor-Beziehung)
- **Gemeinsame Verantwortung** (Joint Controllership)
- **Getrennte Verantwortung** (Controller-to-Controller-Beziehung)

a) Auftragsverarbeitung

Im Bereich der Bürgerforschung wird man, wie bereits beschrieben, in den meisten Fällen jedoch nicht von einer Auftragsverarbeitung ausgehen können, da die Bürgerforscher auf freiwilliger Basis teilnehmen und dabei gerade nicht nur nach Weisung eines Auftraggebers handeln.

Dies schließt allerdings nicht aus, dass z. B. ein **Rechenzentrum als Auftragsverarbeiter** von einer koordinierenden Institution eingeschaltet wird und auch die Bürgerforscher Daten technisch direkt an das Rechenzentrum liefern. Dort sollten die Daten im Sinne einer Reduktion der Komplexität in der Regel aber nur im Auftrag der Institution – und nicht auch der Bürgerforscher – verarbeitet werden.

b) Gemeinsame Verantwortung

> Bei der **gemeinsamen Verantwortung** (Art. 26 DSGVO) legen zwei oder mehrere Verantwortliche gemeinsam Zwecke und wesentliche Mittel der Verarbeitung fest.

Die gemeinsam Verantwortlichen haben in einer Vereinbarung festzulegen, wer welche datenschutzrechtlichen Pflichten erfüllt. Die Vereinbarung muss die tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber den betroffenen Personen gebührend widerspiegeln. Die wesentlichen Inhalte der **Vereinbarung** müssen den betroffenen Personen zur Verfügung gestellt werden. Jede betroffene Person kann ihre Rechte gegenüber jedem einzelnen der Verantwortlichen geltend

---

[17] Mustervereinbarungen zur Auftragsverarbeitung können z. B. hier https://www.bfdi.bund.de/DE/Datenschutz/Datenschutz-GVO/Aktuelles/Aktuelles_Artikel/Muster_Auftragsverarbeitung.html (PDF und DOC) und hier https://www.baden-wuerttemberg.datenschutz.de/datenschutz-in-zeiten-der-krise-handreichungen-des-lfdi-helfen-bei-auftragsverarbeitung-innerhalb-der-eu-und-des-ewr/ (auf Deutsch und Englisch) abgerufen werden.

[18] Ein Musterbeispiel für eine schriftliche Verpflichtung auf den Datenschutz findet sich als Anlage zum Kurzpapier Nr. 19 der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) zur Auslegung der DSGVO: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_19.pdf.

machen. Gleichwohl bleibt zu beachten, dass die Weitergabe von Daten auch zwischen gemeinsam Verantwortlichen eine besonders rechtfertigungsbedürftige Übermittlung darstellt.

Nach der Rechtsprechung des EuGH im bereits oben erwähnten Fall der Datenerhebung durch Zeugen Jehovas ist die gemeinsame datenschutzrechtliche Verantwortlichkeit **weit auszulegen**, sodass bereits die Zurverfügungstellung organisatorischer Hilfsmittel und Empfehlungen für die Vorgehensweise durch eine Institution in der Regel zu einer Mitverantwortung führt.[19] Auch wird in aller Regel im Hinblick auf die verschiedenen Beteiligten an klinischen (Arzneimittel-)Studien davon ausgegangen, dass diese in gemeinsamer Verantwortung agieren: sowohl das Pharmaunternehmen, das als Sponsor auftritt und das Studienprotokoll maßgeblich bestimmt, als auch eine eventuell zur Koordinierung eingeschaltete „Clinical Research Organisation" sowie eine oder mehrere Kliniken, welche die Prüfung mit den betroffenen Patienten bzw. Probanden durchführen.[20]

Diese Vergleichsmaßstäbe sprechen dafür, dass auch im Rahmen der Bürgerforschung, welche durch Institutionen initiiert und koordiniert wird, **regelmäßig eine gemeinsame Verantwortung** von Bürgerforscher und Institution vorliegt. Das Risiko der gesamtschuldnerischen Haftung („einer für alle, alle für einen") von Bürgerforscher und Institution den betroffenen Personen gegenüber müsste in diesem Fall hingenommen werden. Auch wäre eine entsprechende Vereinbarung zur Pflichtenaufteilung gemäß Art. 26 DSGVO abzuschließen. Ein Vertragsmuster hierfür mit kurzer Ausfüllanleitung stellt beispielsweise der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg bereit.[21]

c) Getrennte Verantwortung

> Bei der **getrennten Verantwortung** gelten beide oder mehrere Parteien als jeweils eigenständig Verantwortliche. Diese legen jeweils für sich selbst die Zwecke und die wesentlichen Mittel der Datenverarbeitung fest.

Hier werden die Daten von einem Verantwortlichen an einen anderen Verantwortlichen (Dritten) übermittelt, wobei jeder Verantwortliche Zwecke und wesentliche Mittel seiner jeweiligen Verarbeitung selbst bestimmt. Vertragliche Vereinbarungen sind hierfür allenfalls Indizien. Letztlich maßgeblich sind die tatsächlichen Umstände und Beziehungen der Parteien. Zwar sind in solchen Controller-to-Controller-Beziehungen Vertragsklauseln zum Datenschutz nicht zwingend, aber oft ebenfalls sinnvoll.

Bei getrennter Verantwortung **haftet die übermittelnde Stelle grundsätzlich nicht für einen Datenschutzverstoß durch die empfangende Stelle**, wenn eine Erlaubnis für die Datenübermittlung vorliegt. Diese im Vergleich zur gemeinsamen Verantwortung klare Haftungsabgrenzung hat Vorteile. Allerdings müssen die jeweiligen Voraussetzungen vorliegen, also Zwecke und wesentliche Mittel jeweils eigenständig festgelegt werden.

Dies ist auch im Bereich der Bürgerforschung nicht ausgeschlossen, so wenn Bürgerforscher zunächst eigenständig und ohne Initiierung oder Koordinierung durch eine Institution Daten erheben sowie verarbeiten und diese dann erst nachträglich einer Institution für deren eigenen Zwecke zur Verfügung

---

[19] Zu diesem EuGH-Urteil siehe oben S. 8. In dem Urteil wurde die Organisation der Zeugen Jehovas als zusammen mit den Mitgliedern gemeinsam verantwortlich für die Datenerhebung durch Letztere an der Haustüre von Andersgläubigen eingestuft.
[20] Vgl. das Kurzpapier Nr. 16 der Datenschutzkonferenz zu gemeinsam für die Verarbeitung Verantwortlichen: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf.
[21] LfDI Baden-Württemberg, Mehr Licht! – Gemeinsame Verantwortlichkeit sinnvoll gestalten, 22.05.2019: https://www.baden-wuerttemberg.datenschutz.de/mehr-licht-gemeinsame-verantwortlichkeit-sinnvoll-gestalten/.

stellen. Dann liegt eine klassische Datenübermittlung zwischen zwei eigenständig verantwortlichen Stellen vor.

d) Abgestufte Verantwortung nach Verarbeitungsschritten

Für verschiedene Abschnitte der Datenverarbeitung können aber auch unterschiedliche Verantwortungsmodelle zur Anwendung kommen, **wenn die einzelnen Teile sich** – selbst für die betroffenen Personen – **klar trennen lassen**. So erfolgt zum Beispiel eine strukturierte Datenerhebung durch Bürgerforscher koordiniert von einer Institution typsicherweise in gemeinsamer Verantwortung (Phase 1). Wenn sich die Institution aber vorbehält, im rechtlich zulässigen Rahmen nach Übermittlung (Phase 2) selbst über die weiteren Zwecke und Mittel der Datenverarbeitung zu entscheiden, dann ist die Institution für diese Weiterverarbeitung allein verantwortlich und die Bürgerforscher können insoweit nicht mehr in Haftung genommen werden.

Diese Konstruktion dürfte sich daher häufiger für die institutionell koordinierte Bürgerforschung anbieten. Auch dann wäre der Abschluss einer Vereinbarung über die gemeinsame Verarbeitung angezeigt. In dieser könnte dann auch der **„Übergabepunkt"** sinnvoll und klar definiert werden, ab dem die Institution die alleinige Verantwortung trägt. Auch dieser Punkt wäre den betroffenen Personen in Datenschutzhinweisen zusammen mit den wesentlichen Inhalten der Vereinbarung über die gemeinsame Verarbeitung und den übrigen gesetzlich vorgeschriebenen Punkten transparent zu machen.[22]

VI. Was sind personenbezogene Daten?

Das Datenschutzrecht gilt nach Art. 2 Abs. 1 DSGVO für die Verarbeitung personenbezogener Daten.

> **Personenbezogene Daten** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen (Art. 4 Nr. 1 DSGVO). Nicht erfasst sind anonyme Daten und Daten verstorbener Personen (vgl. Erwägungsgründe 26, 27, 158, 160 DSGVO).

Abbildung 2: Beispiele für personenbezogenen Daten

Der Personenbezug ergibt sich somit daraus, dass sich eine Person aufgrund dieser Daten direkt erkennen lässt (identifizierte Person) oder dass sich die Person in Kombination mit weiteren Informationen

[22] Zu den weiteren Informationspflichten siehe unten S. 23 f.

bestimmen lässt (identifizierbare Person). Mit der ständigen Rechtsprechung des EuGH ist der Begriff des Personenbezugs weit und kontextbezogen zu verstehen.

> In Art. 9 Abs. 1 DSGVO sind zudem **besondere Kategorien personenbezogener Daten** definiert, die als sensibel gelten und deren Verarbeitung daher an besonders strenge Rechtmäßigkeitsvoraussetzungen (Art. 9 Abs. 2 DSGVO) geknüpft ist. Diese Kategorien bestehen aus Daten zur ethnischen Herkunft, zu politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen oder zur Gewerkschaftszugehörigkeit, sowie aus genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung, Gesundheitsdaten oder aus Daten zum Sexualleben.

Von den personenbezogenen Daten müssen **Daten ohne Personenbezug** abgegrenzt werden, da für diese die Vorschriften der DSGVO keine Anwendung finden. Dabei handelt es sich zum einen um Daten, die eine reine Beobachtung von Natur oder Technik darstellen, und zum anderen um Daten, die sich zwar auf Menschen beziehen, aber anonym sind, also keinen Bezug zu einer identifizierten oder identifizierbaren natürliche Person (mehr) haben.

1. Im Allgemeinen: Daten einer identifizierten oder identifizierbaren natürlichen Person

> **Identifiziert** ist eine natürliche Person dann, wenn sie direkt aus den bereits vorhandenen personenbezogenen Daten bestimmt werden kann.
>
> **Beispiele:** Name, Geburtsdatum, Adresse, E-Mail-Adresse, Telefonnummer etc.

Das heißt die Person muss sich von anderen Personen aus einer Gruppe ohne Weiteres eindeutig unterscheiden lassen. Die Identifikation läuft dabei über eindeutig bestimmbare Merkmale ab, welche die Person von der Gruppe unterscheiden und damit individualisieren.

> **Identifizierbar** ist eine natürliche Person dann, wenn sie durch Heranziehung weiterer Informationen bestimmt werden kann.
>
> **Beispiele:** Ermittlung der Identität einer Person durch Verwendung von ergänzenden Informationen wie IP-Adresse, Kfz-Kennzeichen, Personalnummer, Kontonummer, ähnliche Bilder in sozialen Netzwerken, Suchmaschinen für Gesichtserkennung oder weitere nicht ausreichend anonymisierte Daten.

Für die Feststellung, ob eine natürliche Person identifizierbar ist, sind nach Erwägungsgrund 26 DSGVO alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sind alle objektiven Faktoren wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand heranzuziehen, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

Vor diesem Hintergrund sind die **Anforderungen an eine Anonymisierung**, durch welche die Identifizierbarkeit in diesem Sinne ausgeschlossen wird, **recht hoch einzustufen**. Als personenbezogene Daten sind auch pseudonymisierte Daten zu betrachten, die durch Heranziehung zusätzlicher Informationen – insbesondere der Liste oder Vorschrift zur Zuordnung des Pseudonyms – einer natürlichen Person zugeordnet werden können (Erwägungsgrund 26 Satz 2 DSGVO).

2. Daten über den/die Bürgerforscher/in

Im Wege der Bürgerforschung erheben die Bürgerforscher ihre Forschungsdaten zunächst in der Regel selbst. Diese Forschungsdaten beinhalten oft auch deren personenbezogene Daten, welche die Bürgerforscher ohne Weiteres über sich selbst erheben dürfen. Sobald diese Daten aber an andere Stellen übermittelt werden, einschließlich des Bereithaltens einer Abrufmöglichkeit, sind die Regelungen des Datenschutzes auch zu Gunsten der Bürgerforscher zu beachten. Dies gilt unabhängig davon, ob die Bürgerforscher selbst auch Gegenstand bzw. **Objekt** der Forschung sind, so zum Beispiel bei Bürgerforschung im Bereich Gesundheit und Fitness (Stichwort „quantified self"), oder ob sie „nur" **Subjekt** der Forschung sind, beispielsweise wenn sie bei zoologischer Bürgerforschung lediglich Tiere beobachten und diese Beobachtungen bewerten.

Gerade im Hinblick darauf, dass unter den Bürgerforschern die Erhebung von **Bild-, Video- und Tonaufnahmen** mit dem eigenen Smartphone sehr verbreitet ist, generieren sie in den meisten Fällen auch unbewusst personenbezogene Daten, durch welche die Bürgerforscher identifiziert werden können. So wird im Allgemeinen davon ausgegangen, dass Fotografien, auf denen das Gesicht einer Person erkennbar ist, personenbezogen sind.

Ein Personenbezug kann sich aber auch aus sogenannten **Metadaten** ergeben. Dabei handelt es sich um strukturierte Daten, die Informationen über Merkmale anderer Daten enthalten. So können in den Metadaten eines Bildes Informationen wie Kameramodell, Geräte-ID, Startortdaten usw. „versteckt" sein, welche wiederum zu einer Identifizierbarkeit des Bürgerforschers führen könnten. Sofern sich aber singuläre Standortdaten auf den öffentlichen Raum beziehen, wird man allein daraus in der Regel noch keinen Personenbezug ableiten können. Mehr Vorsicht ist dagegen geboten, wenn sich Standortdaten auf ein privates Einfamilienhaus beziehen oder sich aus ihnen ein Bewegungsprofil ableiten lässt.

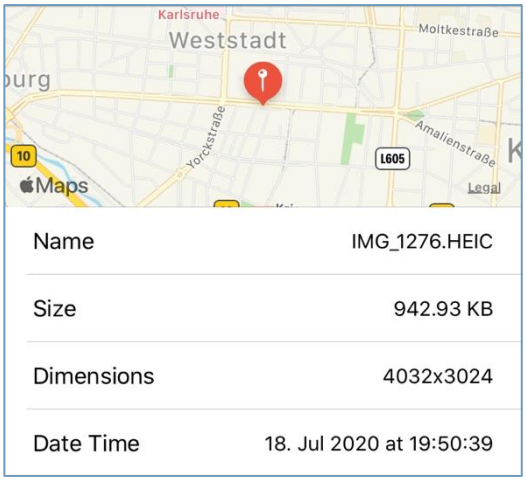

Abbildung 3: Auszug von Metadaten eines Bildes, bei dem Ort und Zeit der Aufnahme erkennbar sind

3. Daten über andere Personen, die Gegenstand oder „Beifang" der Forschung sind

Neben den personenbezogenen Daten der Bürgerforscher können aber auch personenbezogene Daten Dritter erhoben werden. Auf diese finden ebenfalls die datenschutzrechtlichen Vorschriften Anwendung – und zwar bereits bei Erhebung durch die Bürgerforscher.

Personenbezogene Daten Dritter werden im Rahmen der Bürgerforschung unter anderem dann erfasst, wenn sie **Gegenstand der Forschung** sind. Dabei handelt es sich zum Beispiel um Daten zu Personen, die im Rahmen zeitgeschichtlicher Bürgerforschung aus öffentlichen Registern, Zeitungen oder Familienaufzeichnungen erhoben werden.

Im Rahmen der Bürgerforschung können aber auch personenbezogene Daten Dritter erfasst werden, die völlig unbeteiligt an der Forschung sind und daher bloßen **„Beifang"** darstellen. Das ist beispielsweise der Fall, wenn sich Dritte bei der Datenerhebung eines Bildes im Hintergrund aufhalten und dabei Teil des Bildes werden. Innerhalb dieses Bildes kann man diese Personen unter Umständen über ihr Gesicht in offensichtlicherer Weise identifizieren oder unter Heranziehung weiterer Daten durch Anhaltspunkte

wie Standort, Aufnahmezeitpunkt oder Kfz-Kennzeichen identifizierbar machen. Neben Bildern können sich personenbezogene Daten Dritter unter Umständen aber auch aus Stimmen und Gesprächen ergeben, die innerhalb einer Tonaufnahme wahrnehmbar sind. Das wäre der Fall, wenn Bürgerforscher den Gesang einer Nachtigall aufnehmen, im Hintergrund aber ein Gespräch zu verfolgen ist, bei dem die vollständigen Namen der Beteiligten genannt werden.

VII. Welche Grundsätze müssen bei der Verarbeitung solcher Daten für die Bürgerforschung beachtet werden?

Art. 5 DSGVO stellt fundamentale Grundsätze auf, die bei der Verarbeitung personenbezogener Daten von dem Verantwortlichen eingehalten werden müssen.

1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Gemäß Art. 5 Abs. 1 Buchstabe a DSGVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise, also transparent, verarbeitet werden.

a) Rechtmäßigkeit

> Auf **rechtmäßige Weise** in diesem Sinne werden personenbezogene Daten verarbeitet, wenn eine Rechtsgrundlage hierfür existiert. Die Verarbeitung ohne solche Grundlage ist also verboten.

Art. 6 Abs. 1 Satz 1 DSGVO sieht hierfür die folgenden **Rechtsgrundlagen** vor:

a) die wirksame Einwilligung der betroffenen Person,
b) die Erforderlichkeit zur Erfüllung eines Vertrages,
c) die Erforderlichkeit zur Erfüllung rechtlicher Verpflichtungen,
d) die Erforderlichkeit zum Schutz lebenswichtiger Interessen,
e) die Erforderlichkeit zur Wahrnehmung von Aufgaben im öffentlichen Interesse oder
f) die Erforderlichkeit zur Wahrung überwiegender berechtigter Interessen.

Die Rechtsgrundlagen für die Verarbeitung nach Art. 6 Abs. 1 S. 1 Buchstabe c DSGVO (rechtliche Verpflichtung) und Buchstabe e (öffentliche Aufgabe) müssen durch die EU oder die Mitgliedstaaten in ergänzenden Rechtsvorschriften festgelegt werden (Art. 6 Abs. 2, 3 DSGVO). Die Berufung allein auf die DSGVO ist insoweit nicht ausreichend.

Für die Verarbeitung **besonderer Kategorien personenbezogener Daten** (wie Gesundheitsdaten) muss **zusätzlich eine Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO** vorliegen. Für die Forschung kommen hier die ausdrückliche Einwilligung nach Art. 9 Abs. 2 Buchstabe a DSGVO und die Öffnungsklausel zu Gunsten wissenschaftlicher und historischer Forschungszwecke gemäß Buchstabe j in Betracht.

Die Einwilligung als Rechtsgrundlage

> Eine **Einwilligung** der betroffenen Person ist 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).

In Art. 7 DSGVO sind zudem weitere allgemeine Bedingungen für die Wirksamkeit einer Einwilligung enthalten. Ein Formerfordernis besteht insoweit zwar nicht, sodass die Einwilligung auch mündlich erklärt werden kann. Allerdings muss der Verantwortliche nachweisen können, dass die betroffene Person eingewilligt hat (Art. 7 Abs. 1 DSGVO), weshalb bei Rückgriff auf die Einwilligung zumindest eine andere Form der **Dokumentation** notwendig ist, zum Beispiel die elektronische Protokollierung des Anhakens der Checkbox eines Web-Formulars oder die Tonaufzeichnung einer mündlichen Einwilligung. Erfolgt die Einwilligung der betroffenen Person jedoch durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, muss das Ersuchen um Einwilligung in **verständlicher und leicht zugänglicher Form** in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist (Art. 7 Abs. 2 DSGVO). Eine grafische Abgrenzung zu anderen Regelungspunkten eines Dokumentes (wie zu Versicherung oder Aufwendungsersatz für Bürgerforscher) kann zum Beispiel durch einen Rahmen um den Einwilligungstext geschaffen werden.

Auch ist die **Freiwilligkeit** einer Einwilligung kritisch zu hinterfragen, falls eine Leistung an die betroffene Person nur dann erbracht wird, wenn diese eine Einwilligung erteilt, obwohl die Einwilligung für die Leistungserbringung nicht erforderlich ist (Koppelungsprüfung gemäß Art. 7 Abs. 4 DSGVO). Die Freiwilligkeit dürfte vor diesem Hintergrund exemplarisch zu verneinen sein, falls eine Institution Versicherungsschutz für Bürgerforscher nur dann vermittelt, wenn diese in eine Datenverarbeitung einwilligen, die mit dem Versicherungsschutz nichts zu tun hat und auch für das Forschungsprojekt nicht zwingend erforderlich ist. Anders läge der Fall, wenn für den Versicherungsschutz lediglich in die Weitergabe von bestimmten Daten an die Versicherung eingewilligt werden müsste, die Daten dort zur Prüfung des Risikos sowie der Kalkulation der Prämien verarbeitet werden und hierfür auch nötig sind.

In jedem Fall ist zu beachten, dass die betroffene Person das Recht hat, ihre Einwilligung jederzeit zu widerrufen (Art. 7 Abs. 3 DSGVO). Durch den **Widerruf** der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die Einwilligung entfällt mit dem Widerruf jedoch als Rechtsgrundlage für die weitere Verarbeitung, was prinzipiell auch die fortdauernde Speicherung unzulässig macht. Die betroffene Person muss vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt werden. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

Für die **Einwilligung eines Kindes** enthält Art. 8 DSGVO in Bezug auf Dienste der Informationsgesellschaft, wie Online-Dienste oder Smartphone-Apps, weitere Bedingungen. Werden solche Dienste direkt einem Kind – auch wenn es als Bürgerforscher auftritt – angeboten, so ist die Verarbeitung von dessen personenbezogenen Daten rechtmäßig, wenn es das **sechzehnte Lebensjahr** vollendet hat.

Vor dem sechzehnten Geburtstag ist diese Verarbeitung nur rechtmäßig, sofern diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind (den **Erziehungsberechtigten**) oder mit dessen Zustimmung erteilt wird. Der Verantwortliche unternimmt unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde.

Die Mitgliedstaaten können zwar durch Rechtsvorschriften eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf. Von dieser Öffnungsklausel hat in Deutschland der für Dienste der Informationsgesellschaft zuständige Bund jedoch keinen Gebrauch gemacht.

Nach Art. 9 Abs. 2 Buchstabe a DSGVO muss die betroffene Person in die Verarbeitung der besonders **sensiblen personenbezogenen Daten** für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt haben. In Ergänzung zur Einwilligung nach Art. 6 Abs. 1 S. 1 Buchstabe a DSGVO muss die Einwilligung also **ausdrücklich erklärt** werden, wodurch Einwilligungen aufgrund schlüssigen Handelns in diesem Bereich ausgeschlossen sind. Außerdem muss sich die Einwilligung ausdrücklich auf die konkret verarbeitete(n) besondere(n) Kategorie(n) personenbezogener Daten beziehen.

Die DSGVO hat in Erwägungsgrund 33 speziell für die wissenschaftliche Forschung die Möglichkeit der **weiten Einwilligung** („broad consent") geschaffen. Demnach soll es der betroffenen Person erlaubt sein, ihre Einwilligung nicht nur für ganz konkrete Forschungsprojekte, sondern auch für **bestimmte Bereiche der wissenschaftlichen Forschung** zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Dabei soll der Betroffene aber die Gelegenheit erhalten, seine Einwilligung nur für bestimme Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen. Die Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung erfordert außerdem, die Datenverarbeitung für andere als die ursprünglich genannten Vorhaben von einer Ethikkommission und/oder einem Use-and-Access-Komitee freigeben zulassen.[23]

Ist Bürgerforschung wissenschaftliche oder historische Forschung im Sinne der DSGVO?

Vor dem Hintergrund der Privilegierung der wissenschaftlichen Forschung durch die ausnahmsweise Zulässigkeit einer weiten, über einen bestimmten Fall hinausgehenden Einwilligung, stellt sich die Frage, ob Bürgerforschung den Anforderungen wissenschaftlicher (einschließlich historischer) Forschung genügt. Für die Bürgerforschung gilt in Bezug auf die DSGVO hier nichts anderes als für die Forschung im Allgemeinen.

> Die DSGVO sieht selbst vor, dass die Verarbeitung personenbezogener Daten zu **wissenschaftlichen Forschungszwecken** im Sinne dieser Verordnung **weit ausgelegt** werden sollte; eingeschlossen sind Verarbeitungen beispielsweise für die technologische Entwicklung, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung (Erwägungsgrund 159 S. 2 DSGVO).

Dieser weite Ansatz der DSGVO entspricht der **Wissenschaftsfreiheit** nach Art. 13 der EU-Grundrechtecharta, die durch das deutsche Grundgesetz inspiriert wurde. Dementsprechend kann auch die nähere Definition des Bundesverfassungsgerichts hierzu herangezogen werden. Wissenschaft ist demnach jede Tätigkeit, die „nach Inhalt und Form als ernsthafter und planmäßiger Versuch zur Ermittlung von Wahrheit anzusehen ist".[24] Dies gilt im Übrigen auch für die historische Forschung, welche letztlich einen Unterfall der wissenschaftlichen Forschung darstellt.

Das Erfordernis der **Planmäßigkeit** stellt gewisse Mindestanforderungen an die Methodik des Vorgehens. Eine Sammlung von Daten aus Sammelleidenschaft ohne jeden Plan für eine Auswertung wird man daher noch nicht als wissenschaftliche Forschung einordnen können, selbst wenn sich die Datensammlung für wissenschaftliche Zwecke nutzen ließe.

---

[23] Vergleiche dazu auch den Beschluss der Datenschutzkonferenz zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" in Erwägungsgrund 33 der DSGVO vom 03.04.2019: https://www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf.
[24] BVerfG, Beschluss vom 01.02.1978 – 1 BvR 333/75 u.a. (Hessisches Universitätsgesetz).

Der **ernsthaften Suche nach der Wahrheit** würde eine Unterordnung des Forschungszwecks unter wirtschaftliche oder sonstige Zwecke widersprechen. Die Forschung muss insofern unabhängig erfolgen. Dies schließt jedoch eine Verfolgung anderer Zwecke neben oder mit der Forschung ebenso wenig aus wie eine private Finanzierung oder eine wirtschaftliche Verwertung der Ergebnisse. Die lediglich scheinwissenschaftliche Begründung vorgegebener Ergebnisse wäre damit jedoch nicht zu vereinbaren.

Dies gilt grundsätzlich auch für die langfristige Geheimhaltung von Forschungsergebnissen. Denn Forschung ist „letztlich auf Kommunikation und **Publikation** ausgerichtet", so ebenfalls das Bundesverfassungsgericht.[25] Auch setzt sich die EU in Art. 179 Abs. 1 des Vertrages über ihre Arbeitsweise (AEUV) die Schaffung eines europäischen Raums der Forschung zum Ziel, in dem wissenschaftliche Erkenntnisse frei ausgetauscht werden. Dies ermöglicht der „scientific community" eine Überprüfung und Weiterentwicklung dieser Erkenntnisse.[26]

Eine Ausnahme vom Veröffentlichungserfordernis könnte man unter Umständen bei besonders missbrauchsanfälligen Ergebnissen machen, wie solchen zu Kern- oder Biowaffen, gerade sofern Experimente im Haushalt eines Bürgers, beispielsweise mittels der Gen-Schere CRISPR/CAS, für die Allgemeinheit extrem gefährlich wären.[27] Hier könnte ein „Peer Review" der Details dann auf kleinere Zirkel vertrauenswürdiger Experten beschränkt werden. Zur Unterrichtung der Öffentlichkeit über das Gefahrenpotenzial könnte man sich auf die Veröffentlichung einer Zusammenfassung ohne Details beschränken.

Vor diesem Hintergrund ist nicht ersichtlich, warum die **Bürgerforschung** pauschal keine wissenschaftliche Forschung im Sinne der DSGVO darstellen sollte. Die entsprechenden Vorschriften der DSGVO sollen der Wissenschaftsfreiheit und nicht Berufsfreiheit Geltung verschaffen. Der Umstand, dass es sich bei Bürgerforschern nicht um Berufswissenschaftlicher handelt, spielt daher für sich genommen keine Rolle.

Sofern die Bürgerforschung die eben für die **Forschung beschriebenen allgemeinen Bedingungen** erfüllt, stellt sie auch Forschung im Sinne der entsprechenden Vorschriften der DSGVO dar. Zuzugeben ist, dass gerade die Anforderungen an eine planmäßige Methodik und die Veröffentlichung bzw. Transparenzherstellung im Bereich individueller Bürgerforschung nicht immer einfach zu erfüllen sein mögen. Gerade bei Vorhaben, die von Institutionen initiiert und/oder koordiniert werden, sollten sich über die professionelle Unterstützung beim Forschungsdatenmanagement allerdings die entsprechenden Kriterien erfüllen lassen. Auch vor diesem Hintergrund ist die Erstellung eines Datenmanagementplans zu empfehlen, den manche Fördermittelgeber auch vorschreiben und der auch Synergien mit der datenschutzrechtlich vorgeschriebenen Dokumentation birgt.[28]

---

[25] BVerfG, Beschluss vom 01.02.1978 – 1 BvR 333/75 u.a. (Hessisches Universitätsgesetz).

[26] Auch der Kodex der Deutschen Forschungsgemeinschaft (DFG) vom September 2019 zur Sicherung guter wissenschaftlicher Praxis schreibt in seiner Leitlinie 13 die „Herstellung von öffentlichem Zugang zu Forschungsergebnissen" als Voraussetzung für die Förderung durch die DFG grundsätzlich vor. Lediglich im Einzelfall kann es Ausnahmen geben, über welche die Wissenschaftler unabhängig zu entscheiden haben. Der Kodex ist hier abrufbar: https://www.dfg.de/download/pdf/foerderung/rechtliche_rahmenbedingungen/gute_wissenschaftliche_praxis/kodex_gwp.pdf.

[27] Zu dieser Debatte: Stollorz, Wir züchten uns Biowaffen, FAZ.NET, 02.04.2012, https://www.faz.net/aktuell/feuilleton/virenforschung-wir-zuechten-uns-biowaffen-11705662.html.

[28] Nähere Informationen zum Datenmanagementplan: https://www.forschungsdaten.info/themen/informieren-und-planen/datenmanagementplan/. Zur Datenschutz-Dokumentation, insbesondere dem Verzeichnis der Verarbeitungstätigkeiten, siehe unten S. 29.

Gesetzliche Forschungsklauseln als Rechtsgrundlage

Wenn eine Verarbeitung **besonderer Kategorien personenbezogener Daten** für im öffentlichen Interesse liegende wissenschaftliche oder historische Forschungszwecke erforderlich ist, können die EU oder die Mitgliedstaaten nach der Öffnungsklausel in Art. 9 Abs. 2 Buchstabe j DSGVO eine Rechtsgrundlage für diese Verarbeitung schaffen, sofern diese in angemessenem Verhältnis zum verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt sowie angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht. Eine solche Grundlage muss zusätzlich nach herrschender Auffassung aber auch noch mit Art. 6 Abs. 1 DSGVO in Einklang gebracht werden; hier kommt insbesondere Buchstabe e dieser Vorschrift in Betracht, denn entsprechende Forschung ist in der Regel eine Aufgabe, die im öffentlichen Interesse liegt.

Die BRD hat von diesen Öffnungsklauseln mit **§ 27 BDSG** Gebraucht gemacht, der für die Verarbeitung besonderer Kategorien personenbezogener Daten zu Forschungszwecken durch öffentliche Stellen des Bundes sowie nicht-öffentliche Stellen gilt. Auch private Forschung kann einem öffentlichen Interesse dienen, sofern sie die oben beschriebenen Kriterien der Wissenschaftlichkeit erfüllt, also nicht versucht vorgegebene Ergebnisse zu begründen, sondern objektiv und methodisch Erkenntnisse zu generieren und diese mit der „scientific community" zu teilen.

Für öffentliche Stellen der Länder sind jedoch die einschlägigen Regelungen der **Landesdatenschutzgesetze** zu beachten. Auch haben bereichsspezifische Sonderregelungen – wie zum Beispiel das Sozialgesetzbuch für Sozialversicherungen – Vorrang, sodass ein gewisser „Flickenteppich" bei den Forschungsklauseln existiert.[29]

Für die erfassten Stellen sieht **§ 27 Abs. 1 BDSG** vor, dass die Verarbeitung besonderer Kategorien personenbezogener Daten auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke zulässig ist, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die **Interessen des Verantwortlichen** an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung **erheblich überwiegen**. Insofern ist eine qualifizierte Interessenabwägung erforderlich, bei der man nicht immer zu einem erheblichen Überwiegen des Forschungsinteresses gelangen wird. Auch darf der Verantwortliche personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist (§ 27 Abs. 4 BDSG).

Der Verantwortliche hat zudem angemessene und spezifische **Maßnahmen zur Wahrung der Interessen der betroffenen Person** gemäß § 22 Abs. 2 S. 2 BDSG vorzusehen. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören:

1. technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der DSGVO erfolgt,

---

[29] Im Anhang der „Handreichung Datenschutz" des Rats für Sozial- und Wirtschaftsdaten (RatSWD) findet sich z. B. (auf S. 38 f.) eine Übersicht zu den Rechtsgrundlagen, die auf die beim RatSWD akkreditierten Forschungsdatenzentren anwendbar sind. Die Handreichung (2. Auflage 2020) ist hier abrufbar: https://www.ratswd.de/dl/RatSWD_Output8.6_HandreichungDatenschutz_2.pdf.

2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,
3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. Benennung einer oder eines Datenschutzbeauftragten,
5. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
6. Pseudonymisierung personenbezogener Daten,
7. Verschlüsselung personenbezogener Daten,
8. Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
9. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder
10. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der DSGVO sicherstellen.

Für **„normale" personenbezogene Daten** kann allerdings nicht auf § 27 BDSG zurückgegriffen werden. Ein unmittelbarer Rückgriff auf Art. 6 Abs. 1 S. 1 Buchstabe e DSGVO (öffentliches Interesse) scheitert im Anwendungsbereich des BDSG, wenn keine bereichsspezifischen Ergänzungen vorliegen, aber daran, dass der Gesetzgeber diese Öffnungsklausel nicht für die Forschung mit solchen „normalen" Daten genutzt hat. Stattdessen verweist die Begründung zum BDSG insoweit auf **überwiegende berechtigte Interessen** nach Art. 6 Abs. 1 S. 1 Buchstabe f DSGVO. Diese Rechtsgrundlage gilt nach Art. 6 Abs. 1 S. 1 S. 2 DSGVO jedoch nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung. Somit stellt sich für Forschungseinrichtungen des Bundes die Frage, ob diese als Behörden in diesem Sinne zu qualifizieren sind. Allerdings wird der Begriff der Behörde eng ausgelegt und umfasst nicht alle öffentliche Stellen.[30] Behörden sind nur diejenigen öffentlichen Stellen, die mit Befugnissen ausgestattet sind, die über die im Verhältnis zwischen Privatrechtspersonen geltenden Regeln hinausgehen. So darf zum Beispiel die Datenverarbeitung der Gesundheitsämter im Rahmen der verpflichtenden personenbezogenen Verfolgung von Kontakten SARS-CoV-2-Infizierter nicht von einer freien Interessenabwägung abhängen, sondern muss vom Gesetzgeber klarer im Infektionsschutzgesetz geregelt werden.

Öffentliche Forschungseinrichtungen können dagegen regelmäßig wie private Stellen auch auf die Interessenabwägung nach Art. 6 Abs. 1 S. 1 Buchstabe f DSGVO zurückgreifen. Dabei ist allerdings wichtig, dass diese zu Forschungszwecken verarbeiteten personenbezogenen Daten nicht in den Verwaltungsvollzug gelangen und hier zum Nachteil der betroffenen Person verwendet werden. Wenn dies sichergestellt ist, genügt bei „normalen" personenbezogenen Daten allerdings ein einfaches Überwiegen des berechtigten Interesses (an der Forschung) gegenüber den Interessen der betroffenen Person an einem Ausschluss der Verarbeitung.

[30] Das zeigt sich auch darin, dass der abweichende Begriff der „öffentlichen Stelle" zum Beispiel in Art. 37 Abs. 1 Buchstabe a DSGVO gebraucht wird, wonach alle öffentlichen Stellen einen Datenschutzbeauftragten bestellen müssen.

Gerade wenn betroffene Personen in nicht kompromittierenden Situationen mit ihren „normalen" Daten nur **„Beifang" der Datenerhebung** sind, so zum Beispiel Beiwerk im Hintergrund von Film- oder Fotoaufnahmen, wird man dies häufig auf berechtigte Interessen stützen können, wenn dafür Sorge getragen wird, dass in weiteren Verarbeitungsschritten auch dieser unnötige Personenbezug so weit wie möglich reduziert oder gar ausgeschlossen wird. In solchen „Beifang"-Situationen wäre die Einholung einer Einwilligung im Gegensatz zur Verarbeitung der Daten der Bürgerforscher oder von ausgewählten Probanden ohnehin deutlich erschwert, falls überhaupt möglich.

Geeignete Garantien

Unabhängig davon, ob Forschungszwecke nun auf Grundlage einer Einwilligung oder einer gesetzlichen Erlaubnis einschließlich der zur Interessenabwägung verfolgt werden, muss die entsprechende Verarbeitung personenbezogener Daten geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß Art. 89 Abs. 1 DSGVO unterliegen. Mit diesen Garantien wird sichergestellt, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Zu diesen Maßnahmen kann die **Pseudonymisierung** gehören, sofern es möglich ist, die Zwecke auf diese Weise zu erfüllen. Wenn die Forschungszwecke durch eine Weiterverarbeitung, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, erfüllt werden können, müssen diese Zwecke auf diese Weise erfüllt werden, weshalb dann eine **Anonymisierung** vorzunehmen ist. Häufig wird aber jedenfalls in einer frühen Forschungsphase eine Pseudonymisierung eher mit den Forschungszwecken zu vereinbaren sein als eine Anonymisierung.

b) Treu und Glauben

> Der Grundsatz von **Treu und Glauben** setzt die Gewährleistung einer fairen Verarbeitung voraus.
>
> **Beispiel:** Wird die Einwilligung für eine Verarbeitung vom Verantwortlichen erbeten, aber von der betroffenen Person abgelehnt, so darf nicht die exakt gleiche Verarbeitung auf gesetzlicher Grundlage durchgeführt werden. Dies würde als widersprüchliches Verhalten gegen diesen Grundsatz verstoßen.

Dieser Grundsatz verlangt vor allem, dass auch die „**vernünftigen Erwartungen**" der betroffenen Person berücksichtigt werden (vgl. Erwägungsgrund 47 DSGVO). Dies gilt insbesondere bei der Interessenabwägung nach Art. 6 Abs. 1 S.1 Buchstabe f, Art. 9 Abs. 2 Buchstabe j DSGVO bzw. § 27 BDSG oder ähnlichen Rechtsgrundlagen.

Daneben können diese Erwartungen und der faire Umgang mit ihnen auch bei der Fragen nach der Vereinbarkeit eines neuen Verarbeitungszwecks mit dem sich davon unterscheidenden Erhebungszweck der Daten eine Rolle spielen.[31] Eine über die genannten Fälle hinausgehende eigenständige Bedeutung dieses Prinzips ist jedoch selten.

---

[31] Siehe dazu auch unten die Ausführungen zur Zweckbindung und Zweckvereinbarkeit auf S. 23 f.

c) Transparenz

Der Grundsatz der **Transparenz** setzt voraus, dass die betroffene Person bestimmten Informationen zur Verarbeitung ihrer personenbezogenen Daten leicht zugänglich, verständlich und in klarer und einfacher Sprache abgefasst erhält.

Für die Erhebung von personenbezogenen Daten bei betroffenen Personen trifft den Verantwortlichen daher eine **Informationspflicht** (Art. 12, 13 DSGVO). Demnach muss der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mitteilen:

Information der betroffenen Person (Art. 12 ff. DSGVO)

Verantwortlicher und Ansprechpartner/Kontaktdaten

- Name und Kontaktdaten des Verantwortlichen (einschließlich ladungsfähiger Anschrift)
- Kontaktdaten des Datenschutzbeauftragten (nicht zwingend der Name)

Beschreibung der Verarbeitung personenbezogener Daten

- Kategorien von Daten
- Quellen der Daten (bei Erhebung bei Dritten und nicht der betroffenen Person selbst)
- Zwecke und Rechtsgrundlagen der Verarbeitung
- Kategorien von Empfängern
- (geplante) Übermittlung in Drittland außerhalb des Europäischen Wirtschaftsraums (= EU + Island, Liechtenstein und Norwegen)
- Dauer der Speicherung, zumindest Kriterien für deren Festlegung
- Angabe, ob die Datenbereitstellung gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsschluss erforderlich ist
- Bestehen einer automatisierten Einzelentscheidung (wenn eine solche durchgeführt wird)

Rechte des Betroffenen

Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch in bestimmten Fällen (Art. 21 DSGVO), Widerruf einer ggf. erteilten Einwilligung, Beschwerde bei der Datenschutz-Aufsichtsbehörde.

Informationspflichten bestehen grundsätzlich nach Art. 14 DSGVO auch dann, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden. Die Inhalte entsprechend denjenigen nach Art. 13 DSGVO zur Erhebung bei der betroffenen Person, ergänzt um die Angabe der Quelle der Daten – wie in der obigen Übersicht bereits enthalten.

Allerdings enthält Art. 14 Abs. 5 DSGVO im Gegensatz zu Art. 13 DSGVO einige **Ausnahmen** von der Informationspflicht. Eine solche Ausnahme liegt nach Art. 14 Abs. 5 Buchstabe b DSGVO vor, wenn die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde. Dies gilt insbesondere für die Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken oder für statistische Zwecke vorbehaltlich der in Art. 89 Abs. 1 DSGVO genannten Bedingungen und Garantien oder soweit Informations- bzw. Benachrichtigungspflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt. In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit.

Allerdings stellt zum Beispiel die gezielte Fotografie einer bestimmten Person in der Regel eine Erhebung bei dieser dar, sodass Art. 13 DSGVO und nicht Art. 14 DSGVO mit seinen Ausnahmen anwendbar ist. Beim **Fotografieren von großen Menschenmengen oder Menschen als Beiwerk** von anderen Abbildungen ist es jedoch gut vertretbar, auf Art. 14 DSGVO und seine Ausnahmen zurückzugreifen.[32] Hier ist es nach Art. 11 DSGVO regelmäßig auch nicht erforderlich, als Beiwerk im Hintergrund eines Fotos abgebildete Menschen anzusprechen und diese gegebenenfalls zu identifizieren, um ihnen Datenschutzhinweise zukommen zu lassen. Denn nach Art. 11 Abs. 1 DSGVO ist ein Verantwortlicher nicht verpflichtet zur bloßen Einhaltung der DSGVO zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren, wenn für die Zwecke, für die er Daten verarbeitet, die Identifizierung der betroffenen Person nicht erforderlich ist.

Auch in diesen Fällen sollten die Bilddaten des „Beiwerks", die zwar nicht identifiziert, bei Erkennbarkeit des Gesichtes oder anderer eindeutiger Merkmale aber doch identifizierbar und damit personenbezogen sind, so früh wie möglich, spätestens aber vor Veröffentlichung anonymisiert, also effektiv verpixelt oder geschwärzt werden.

Ebenfalls ist daran zu denken, auf einer **Projektwebsite Datenschutzinformationen** auch für als Beiwerk betroffene Personen bereitzustellen. Auf diese Informationen könnte man betroffene Personen auch verweisen, die den fotografierenden Bürgerforscher gegebenenfalls auf die Fotografie ansprechen.

2. Zweckbindung, Zweckvereinbarkeit und Weiterverarbeitung für die Forschung

Mit den Prinzipen der Zweckbindung und der Zweckvereinbarkeit soll die Verarbeitung personenbezogener Daten überschaubar und kontrollierbar werden.

> Gemäß Art. 5 Abs. 1 Buchstabe b DSGVO ist die **Erhebung personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke** gestattet. Es müssen also vom Verantwortlichen ein oder mehrere Zwecke bereits vor oder bei Erhebung festgelegt werden. Die anschließende Verarbeitung ist dann an diese Zwecke gebunden (**Zweckbindung**). Eine Weiterverarbeitung zu anderen Zwecken ist prinzipiell untersagt, es sei denn, diese Zwecke sind mit den Erhebungszwecken vereinbar (**Zweckvereinbarkeit**).

Eine Weiterverarbeitung für wissenschaftliche oder historische Forschungszwecke gilt, sofern Garantien gemäß Art. 89 Abs. 1 DSGVO bestehen, allerdings nicht als unvereinbar mit den ursprünglichen Zwecken (Art. 5 Abs. 1 Buchstabe b Halbsatz 2 DSGVO). Das heißt, dass die Weiterverarbeitung von ursprünglich zu anderen Zwecken (zum Beispiel der Versicherungsregulierung von Schäden durch Astschlag) erhobenen Daten für Forschungszwecke (sogenannte **Sekundärnutzung**, beispielsweise zur Analyse der Auswirkungen des Klimawandels auf Stadtbäume) vor dem Hintergrund des Grundsatzes der Zweckbindung per Gesetz keiner besonderen Vereinbarkeitsprüfung bedarf.[33]

---

[32] Hierzu und zum Rest des Absatzes: Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Vermerk: Rechtliche Bewertung von Fotografien einer unüberschaubaren Anzahl von Menschen nach der DSGVO außerhalb des Journalismus, Stand: März 2018, S. 5 ff., https://datenschutz-hamburg.de/assets/pdf/Vermerk_Fotografie_DSGVO.pdf.

[33] Ein möglicher Anwendungsfall dieser Überlegungen könnten das Citizen Science-Projekt „TreeChecker" sein: https://www.buergerschaffenwissen.de/projekt/treechecker-welche-strassenbaeume-fuer-die-stadt-der-zukunft.

Erleichterung der Wiederverwendbarkeit nach den FAIR-Prinzipien

Diese Privilegierung der Zweckänderung hin zur Forschung bzw. zu anderen als den ursprünglich vorgesehenen Forschungszwecken erleichtert auch die Wiederverwendbarkeit von Forschungsdaten. Diese Wiederverwendbarkeit findet sich unter anderem in den von der Open Science und letztlich auch der internationalen Citizen Science Community geforderten FAIR-Prinzipien. Die FAIR-Prinzipien bilden die Grundlage für eine disziplinierte und projektübergreifende Weiterverarbeitung von Daten. Hinter dem Akronym „FAIR" verbirgt sich ein Anforderungsprofil zum Umgang von Forschungsdaten, das folgenden Prinzipien folgt: Auffindbarkeit (**Findable**), Zugänglichkeit (**Accessible**), Interoperabilität (**Interoperable**) und Wiederverwendbarkeit (**Reusable**).[34]

Streitfrage: Eigenständige Rechtsgrundlage für die Weiterverarbeitung zur Forschung nötig?

Selbst unter Aufsichtsbehörden ist allerdings umstritten, ob die entsprechende Weiterverarbeitung zu dem geänderten, wenn auch vereinbaren Forschungszweck wegen des selbständigen Grundsatzes der Rechtmäßigkeit einer eigenständigen Rechtsgrundlage bedarf. Dagegen spricht insbesondere Erwägungsgrund 50 S. 2 DSGVO, nach welchem im Fall der Vereinbarkeit „keine andere gesonderte Rechtsgrundlage erforderlich" ist „als diejenige für die Erhebung der personenbezogenen Daten". Dieser Erwägungsgrund hat allerdings eine geringere Bindungswirkung als die eigentlichen Artikel der DSGVO und er wird teilweise als Redaktionsfehler bzw. Überbleibsel bezeichnet, der noch auf eine Entwurfsfassung der DSGVO Bezug nimmt. Auch werden Bedenken ins Feld geführt, ob eine Weiterverarbeitung ohne eigene Rechtsgrundlage auch in Fällen der Vereinbarkeit den gebotenen Grundrechtsschutz gewährleisten kann.

Im Ergebnis mag zwar der Verzicht auf eine gesonderte Rechtsgrundlage bei Zweckvereinbarkeit vertretbar sein, ist jedoch nicht der **sicherste Weg**. Sicherer wäre eine **eigene Rechtsgrundlage** für den Forschungszweck wie die Einwilligung der betroffenen Person oder eine gesetzliche Erlaubnis wie Art. 6 Abs. 1 S. 1 Buchstabe f DSGVO (einfache Interessenabwägung) oder § 27 BDSG (erhebliches Überwiegen bei sensiblen Daten). In jedem Fall dürfte eine neue Rechtsgrundlage erforderlich sein, wenn Daten von der ursprünglich erhebenden Stelle (zum Beispiel dem Bürgerforscher) an eine andere verantwortliche Stelle (wie eine koordinierende Institution) weitergegeben werden, denn dann würde die reine Weiterverarbeitung verlassen und es fände eine neue Erhebung, nämlich durch die zuletzt genannte Stelle statt.

3. Datenminimierung, Pseudonymisierung und Anonymisierung

> Nach dem Grundsatz der **Datenminimierung** (Art. 5 Abs. 1 Buchstabe c DSGVO) müssen personenbezogene Daten für den Verarbeitungszweck erheblich, diesem angemessen und auf das notwendige Maß beschränkt sein.

Das heißt, dass die Datenerhebung vom Umfang auf das Minimum beschränkt sein muss, das zur Erfüllung des rechtmäßigen Zwecks erforderlich ist. Gefordert ist dabei in der Regel jedoch kein absolutes Minimum, sondern lediglich eine **verhältnismäßige Handhabung der Daten**. Dies lässt sich aus Erwägungsgrund 39 zur DSGVO ableiten, wonach personenbezogene Daten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann.

---

[34] TU Wien, FAIR-Prinzipien: https://www.tuwien.at/forschung/fti-support/forschungsdaten/forschungsdatenmanagement/fair-prinzipien/.

Dies gilt sowohl für die Auswahl und den Umfang der personenbezogenen Daten als auch für Art und Umfang der Verarbeitung dieser Daten.

Mögliche Verfahren zur Datenminimierung stellen neben der gezielten und nicht ausufernden Auswahl unmittelbar personenbezogener Daten auch Pseudonymisierung und Anonymisierung als Verfahren zur Reduktion oder gar zum Ausschluss des Personenbezuges dar.

> Unter **Pseudonymisierung** versteht die DSGVO 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 handelt es sich somit um einen Verarbeitungsvorgang, bei dem die personenbezogenen Identifikationsmerkmale (zum Beispiel Name oder Adresse) aus dem Datensatz durch Pseudonyme ersetzt werden. Im Ergebnis können ohne die Hinzuziehung zusätzlicher Informationen die Daten nicht mehr einer spezifischen betroffenen Person zugeordnet werden. Es bleibt auf der einen Seite nur der **pseudonymisierte Datensatz** ohne identifizierende Merkmale übrig, sodass eine Identifizierung des ursprünglichen Betroffenen aus diesem Datensatz heraus nicht mehr möglich ist.

Auf der anderen Seite sind die **zusätzlichen Informationen**, also der ergänzende Datensatz mit der Zuordnung des Pseudonyms zu den identifizierenden Daten oder die Rechenvorschrift zur Zuordnung, **technisch und organisatorisch abgeschottet zu verarbeiten**. Die Forscher dürfen im Regelbetrieb keinen Zugriff auf diese haben. Auch ist an die Etablierung eines Vier-Augen-Prinzips für den Zugriff auf die Zuordnung der identifizierenden Daten von Probanden zu denken.

Sinn und Zweck der Pseudonymisierung liegt in der Senkung von Verarbeitungsrisiken. Aufgrund der Wiederherstellbarkeit pseudonymisierter Daten fallen diese im Gegensatz zu anonymisierten Daten weiterhin unter die **personenbezogenen Daten** (Erwägungsgrund 26 S. 2 DSGVO).

Eine Pseudonymisierung sollte im Rahmen wissenschaftlicher Forschung **möglichst frühzeitig erfolgen** (vgl. Art. 89 Abs. 1 DSGVO, § 27 Abs. 1 S. 2 in Verbindung mit § 22 Abs. 2 S. 2 Nr. 5 BDSG). Einige Landesdatenschutzgesetze schreiben die Pseudonymisierung für Forschungsvorhaben sogar in jedem Fall vor (so zum Beispiel § 13 Abs. 2 S. 2, 3 LDSG Baden-Württemberg).

> Bei der **Anonymisierung** werden die personenbezogenen Daten derart verändert, dass sie sich nicht mehr auf eine identifizierte oder identifizierbare Person beziehen (Erwägungsgrund 26 S. 5 DSGVO).

Die Anonymisierung umfasst im weiteren Sinne auch die **Aggregation**, also die Aufsummierung und gegebenenfalls Durchschnittsbildung der Merkmale von verschiedenen betroffenen Personen. Im engeren Sinne gehören zur Anonymisierung Methoden der **Generalisierung**, so zum Beispiel, wenn statt dem genauen Alter einer betroffenen Person (etwa 45) ein Intervall (40 bis 50 Jahre) angegeben wird, oder der Vergröberung durch Unterdrückung (**Suppression**) andere Details wie des Geburtstages (13.08.1961) und die bloße Angabe des Geburtsjahres (1961), gegebenenfalls samt Monat (08.1961), aber nicht des Tages. Standortdaten könnte man beispielsweise zu größeren Gebieten vergröbern wie Mobilfunkzellen, ohne Angabe des exakten GPS-Standortes. Auch kann man an den Einbau von

Zufallsfehlern durch **Permutation** (Durcheinanderwürfeln von Merkmalsausprägungen) oder sonstige Veränderung denken.

Wichtig ist, dass die Methoden so eingesetzt und gegebenenfalls kombiniert werden, dass sämtliche offensichtlichen Identifikatoren und möglicherweise einsetzbaren Quasi-Identifikatoren so verschleiert werden, dass **nach allgemeinem Ermessen eine Re-Identifizierung äußerst unwahrscheinlich** wird. Die so verarbeiteten, anonymisierten Daten enthalten somit keine direkten oder indirekten Identifikationsmerkmale der betroffenen Personen mehr, weshalb sie prinzipiell nicht den Regelungen des Datenschutzes unterfallen.[35]

Allerdings muss bei der Anonymisierung die **technologische Entwicklung** berücksichtigt werden, wodurch ursprünglich anonymisierte Daten in Zukunft doch wieder re-identifiziert werden könnten. Daher ist im Zeitverlauf zu prüfen, ob nach Anonymisierung verbliebene komplexe Einzeldatensätze, auch wenn diese keine offensichtlichen Identifikatoren mehr enthalten, angesichts der technologischen Entwicklung und der zunehmenden Verfügbarkeit ergänzender Datenquellen doch wieder identifizierbar werden – dann würde die DSGVO auch wieder volle Geltung beanspruchen.

In allen Fällen, in denen wissenschaftliche Forschungszwecke durch eine Weiterverarbeitung, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, erfüllt werden können, werden diese Zwecke auf diese Weise erfüllt (Art. 89 Abs. 1 S. 4 DSGVO). Insofern besteht also eine **Pflicht zur Anonymisierung**, soweit die Forschungszwecke dadurch nicht vereitelt werden.

4. Richtigkeit der Daten

> Nach dem Grundsatz der **Richtigkeit** müssen personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neusten Stand sein (Art. 5 Abs. 1 Buchstabe d DSGVO).

Der Verantwortliche hat daher alle angemessenen Maßnahmen zu treffen, personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, **unverzüglich zu löschen oder zu berichtigen**. Darüber hinaus hat er die betroffene Person gemäß Art. 16 DSGVO das Recht falsche, das heißt unzutreffende persönliche Informationen, einschließlich unvollständiger Daten, berichtigen zu lassen. Dieser Grundsatz deckt sich ohne Weiters mit den Zwecken wissenschaftlicher Forschung.

5. Zeitliche Speicherbegrenzung vs. Sicherung guter wissenschaftlicher Praxis

> Nach dem Grundsatz der **Speicherbegrenzung** dürfen personenbezogene Daten **nur so lange** gespeichert und verarbeitet werden, **wie es für die Verarbeitungszwecke erforderlich** ist (Art. 5 Abs. 1 Buchstabe e DSGVO).

Art. 5 Abs. 1 Buchstabe e DSGVO fordert diese zeitliche Speicherbegrenzung aber ausdrücklich nur für Daten in einer Form, die die Identifizierung der betroffenen Personen ermöglicht. Wenn die Daten effektiv anonymisiert wurden, also nicht mehr personenbezogen sind, dürfen sie auch länger gespeichert werden. Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat anerkannt, dass die Anonymisierung ein sogenanntes „**Löschungssurrogat**" darstellt, also an die Stelle der sonst nötigen Löschung zum Ende der begrenzten Speicherdauer treten kann.[36]

---

[35] Zur Anonymisierung siehe auch das unten in Fußnote 36 auf S. 27 erwähnte Positionspapier des BfDI.

[36] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, Stand: 02.06.2020, S. 8 f., abrufbar unter

Selbst personenbezogene Daten dürfen allerdings **länger gespeichert** werden, soweit diese Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von der DSGVO zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für wissenschaftliche und historische Forschungszwecke gemäß Art. 89 Abs. 1 DSGVO verarbeitet werden. Diese Ausnahme vom Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 Buchstabe e Halbsatz 2 DSGVO soll die Nachprüfbarkeit insbesondere veröffentlichter Forschungsergebnisse wie auch eine weitere Nutzung der Primärdaten für weitere Forschungsprojekte oder langfristige Studien zu ermöglichen.

So sehen auch die Erläuterungen der **Deutschen Forschungsgemeinschaft** (DFG) im Hinblick auf ihre Leitlinie 17 zur Sicherung der guten wissenschaftlichen Praxis Folgendes vor:[37]

> „Wenn wissenschaftliche Erkenntnisse öffentlich zugänglich gemacht werden, werden die zugrunde liegenden Forschungsdaten (in der Regel Rohdaten) – abhängig vom jeweiligen Fachgebiet – in der Regel für einen Zeitraum von zehn Jahren zugänglich und nachvollziehbar in der Einrichtung, wo sie entstanden sind, oder in standortübergreifenden Repositorien aufbewahrt. In begründeten Fällen können verkürzte Aufbewahrungsfristen angemessen sein; die entsprechenden Gründe werden nachvollziehbar beschrieben. Die Aufbewahrungsfrist beginnt mit dem Datum der Herstellung des öffentlichen Zugangs."

Allerdings darf die Speicherung **nicht zu einer unbegrenzten Vorratsdatenhaltung führen**, das heißt, dass der künftige wissenschaftliche Zweck, der die Einhaltung erforderlich macht, nach der jeweiligen Wissenschaftsdisziplin und dem konkreten Forschungskontext absehbar sein muss. Auch sofern eine längere Speicherung erforderlich ist, ist der Grundsatz der Datenminimierung zu beachten und damit regelmäßig eine Pseudonymisierung durchzuführen. Auch ist die Notwendigkeit der Speicherung regelmäßig zu überprüfen.

6. Integrität und Vertraulichkeit, technische und organisatorische Sicherheitsmaßnahmen

Nach dem Grundsatz der **Integrität und Vertraulichkeit** sind personenbezogene Daten in einer Weise zu verarbeiten, die eine **angemessene Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung **durch geeignete technische und organisatorische Maßnahmen** (Art. 5 Abs. 1 Buchstabe f DSGVO).

Dieser Grundsatz wird vor allem durch Art. 32 DSGVO zur Sicherheit der Verarbeitung konkretisiert. Demnach hat der Verantwortliche oder sein Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein **dem Risiko angemessenes Schutzniveau** zu gewährleisten. Diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

1. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

---

https://www.bfdi.bund.de/DE/Infothek/Transparenz/Konsultationsverfahren/01_Konsulation-Anonymisierung-TK/Positionspapier-Anonymisierung-DSGVO-TKG.html. Allerdings fordert der BfDI auch eine Rechtsgrundlage für die Anonymisierung (S. 5 ff.).

[37] Zu diesen Leitlinien der DFG siehe schon oben Seite 18, Fußnote 26.

2. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
3. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
4. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der sicheren Verarbeitung.

Art. 25 DSGVO sieht darüber hinaus Datenschutz durch Technikgestaltung („**privacy by design**") und datenschutzfreundliche Voreinstellungen („**privacy by default**") vor. Diese Vorschrift verpflichten den Verantwortlichen nach Möglichkeit schon bei der Anschaffung oder Entwicklung von (Informations-) Technik und deren Konfiguration darauf zu achten, dass mit dieser Technik die datenschutzrechtlichen Grundätze umgesetzt werden können. Im Rahmen der Bürgerforschung dürfte diese Verpflichtung vor allem von den beteiligten Institutionen erfüllt werden können.

Im Hinblick auf das EuGH-Urteil zur Unwirksamkeit des EU-U.S. Privacy Shields sollten diese Institutionen daher auch **Zurückhaltung bei der Nutzung der Cloud-Dienste von US-Anbietern** an den Tag legen.[38] Denn diese können aufgrund der abweichenden Rechtslage in den USA auch bei Verwendung der Standardvertragsklauseln der EU-Kommission zur Auftragsverarbeitung nicht ohne Weiteres ein der DSGVO entsprechendes Datenschutzniveau gewährleisten. Zusätzlich zu den Standardvertragsklauseln sind daher, sollen doch die Dienste von US-Anbietern zur Verarbeitung personenbezogener Daten im Anwendungsbereich der DSGVO genutzt werden, ergänzende Schutzmaßnahmen wie beispielsweise die Pseudonymisierung noch außerhalb des Zugriffs der US-Anbieter zu erwägen und jedenfalls bei sensiblen Daten auch zu ergreifen.

Zudem stellen der Verantwortliche und der Auftragsverarbeiter sicher, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet. Dies setzt neben Schulungen und anderen **Sensibilisierungsmaßnahmen** regelmäßig eine sogenannte Verpflichtungserklärung voraus.[39]

Auch wenn Bürgerforscher regelmäßig nicht wie Angestellte im hier verwandten Sinne den Institutionen der Bürgerforschung unterstellt sind, bietet sich doch – in der Regel mit Ausnahme der Weisungsabhängigkeit – eine Verpflichtung auf den Datenschutz und weitere Informations- und Sensibilisierungsmaßnahmen der Institutionen für die Bürgerforscher an.

7. Rechenschaftspflicht und Dokumentation

> Gemäß Art. 5 Abs. 2 DSGVO ist der **Verantwortliche** für die Einhaltung der bereits genannten Grundsätze verantwortlich und muss deren Einhaltung auch nachweisen können (**Rechenschaftspflicht**).

Ziel der Regelung ist es, die Verantwortlichen in die Pflicht zu nehmen, wenn auch nicht nur, so doch insbesondere im Hinblick auf den Nachweis der erteilten Einwilligung des Betroffenen oder das Vorliegen einer anderen Rechtsgrundlage für den Verarbeitungsvorgang.

---

[38] EuGH, Urteil vom 16.07.2020, Az. C-311/18 (Schrems II).
[39] Zur Verpflichtungserklärung siehe bereits oben S. 11 und Fußnote 18.

Eine gute Möglichkeit zur Erfüllung der Nachweispflicht stellt das **Verzeichnis von Verarbeitungstätigkeiten** dar (Erwägungsgrund 82 S. 1 DSGVO). Dieses Verzeichnis muss nach Art. 30 Abs. 1 DSGVO ohnehin für jeden Verantwortlichen und jedes Verfahren der Verarbeitung personenbezogener Daten folgende Angaben enthalten:

- Name & Kontaktdaten des Verantwortlichen und, falls vorhanden, des Datenschutzbeauftragten
- Zweck der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und personenbezogener Daten
- Kategorien von Empfängern
- gegebenenfalls Übermittlungen an ein Drittland oder internationale Organisationen
- so weit wie möglich die vorgesehen Fristen für die Löschung der Daten
- so weit wie möglich eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO.

Das Verzeichnis kann über diese Pflichtinhalte hinaus zum Beispiel auch um Angaben zur Rechtsgrundlage einer Verarbeitung erweitert werden. Zudem sind die erforderlichen **Interessenabwägungen**, insbesondere zur Rechtmäßigkeit (im Rahmen von Art. 6 Abs. 1 S. 1 Buchstabe f DSGVO, § 27 BDSG oder vergleichbaren Vorschriften), zumindest in Textform mit Ergebnis und wesentlichen Gründen **zu dokumentieren**. Auch diese Dokumentation kann als Anlage zum entsprechenden Eintrag in das Verzeichnis der Verarbeitungstätigkeiten aufgenommen werden.

Zudem muss bei jeder Verarbeitung das Risiko für die Rechte und Freiheiten der betroffenen Personen einer ersten Bewertung zugeführt werden (sogenannte Schwellwertanalyse). Ergibt sich hier trotz Beachtung der üblichen Datenschutzmaßnahmen ein hohes Risiko, muss eine formale **Datenschutz-Folgenabschätzung** nach Art. 35 DSGVO durchgeführt werden. Bei der Frage, wann ein solches hohes Risiko vorliegt, hilft neben den Kriterien in Art. 35 Abs. 1 und Abs. 3 DSGVO insbesondere auch die sogenannte Positivliste der zuständigen Aufsichtsbehörde nach Abs. 4 dieser Vorschrift. Darin werden Verfahren etwas konkreter beschrieben, bei denen aus Sicht der Aufsichtsbehörde eine Datenschutz-Folgeabschätzung zwingend erfolgen muss. Die deutschen Aufsichtsbehörden haben immerhin für den nicht-öffentlichen Bereich eine solche Positivliste untereinander abgestimmt.[40] Bei Durchführung der Folgenabschätzung müssen Risiken für die betroffenen Personen nicht nur heuristisch, sondern systematisch identifiziert und einzeln bewertet werden. Gleiches gilt für getroffene und eventuell noch zu treffende Schutzmaßnahmen.[41] Das Ergebnis und die wesentlichen Gründe dieser Folgenabschätzung sind zu dokumentieren.[42] Verbleibt auch nach dieser Abschätzung ein hohes Risiko, ist die zuständige Aufsichtsbehörde nach Art. 36 DSGVO zu konsultieren.

---

[40] Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO der Datenschutzkonferenz für den nicht-öffentlichen Bereich: https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf (Version 1.1, 17.10.2018). Für den öffentlichen Bereich muss die Positivliste bei der jeweiligen Aufsichtsbehörde gesucht werden.

[41] Zum Vorgehen: Forum Privatheit, White Paper „Datenschutz-Folgenabschätzung", Ein Werkzeug für einen besseren Datenschutz, 3. Auflage 2017, abrufbar unter https://www.forum-privatheit.de/datenschutz-folgenabschaetzung/.

[42] Ein Beispiel für eine vom BfDI für ausreichend befundene Datenschutz-Folgenabschätzung ist die für die Corona-Warn-App (https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf). Der Umfang von 110 Seiten mit Deckblatt ist hier aber wohl auch der gesellschaftlichen Breitenwirkung der App in seinem sensiblen Umfeld geschuldet.

VIII. Was ist bei Smartphone-Apps als Mittel der Bürgerforschung zu beachten?

Als Mittel zur Datenerhebung finden zunehmend Smartphones sowie Wearables und andere Sensoren, welche nicht für die Forschung im engeren Sinne entwickelt wurden, bei Bürgerforschern Anwendung. Dabei findet die Datenerhebung oft durch Apps statt. Durch Sensoren lassen sich eine Vielzahl verschiedener Merkmale mit hoher zeitlicher und räumlicher Auflösung erfassen, die in manchen Kombinationen zu einer **höheren Wahrscheinlichkeit der Identifizierung** bei einer erfassten Person führen können. Auch für diese Datenverarbeitung haben die Bürgerforscher und die initiierenden bzw. koordinierenden Institutionen die allgemeinen Grundsätze der DSGVO einzuhalten, welche vorliegend in dieser Beziehung veranschaulicht werden sollen.[43]

1. Datenerhebung und -verarbeitung durch den/die Bürgerforscher/in mittels App

Durch die Datenerhebung und der oft automatisch stattfindenden Datenverarbeitung durch Smartphones, werden neben den eigentlichen Daten für die Forschung, die meist dritte Personen betreffen, oft auch Informationen zu den Bürgerforschern und gegebenenfalls ihres persönlichen Umfelds erfasst (beispielsweise durch beinhaltete Metadaten). Dabei kann die **Datenerhebung lokal auf dem Smartphone** auf zweierlei Arten erfolgen:

- Mit Mitteln des Betriebssystems oder von Standard-App statt, indem der Bürgerforscher zum Beispiel ein Foto über die darauf befindliche Kamera-App aufnimmt.
- Der Bürgerforscher erhebt die Daten direkt durch die App der initiierenden/koordinierenden Institution, indem bspw. die Möglichkeit zur Aufnahme eines Bildes direkt in der App integriert ist.

Solange lediglich die **Daten der Bürgerforscher** lokal auf ihrem Smartphone ihre eigenen Daten verarbeiten, ist die datenschutzrechtlich in der Regel unproblematisch und kann noch unter die eingangs angesprochenen Haushaltsausnahme der DSGVO fallen. Allein bei dieser Verarbeitung dürfte es jedoch eher selten bleiben.

Schwieriger gestaltet sich der Fall, wenn **personenbezogene Daten Dritter** erhoben werden. Wenn hier keine Einwilligung praktikabel ist, muss man eine Interessenabwägung nach den jeweils einschlägigen gesetzlichen Vorschriften durchführen. Wenn die Daten Drittbetroffener nur zufälligen „Beifang" der eigentlich gewünschten nicht personenbezogenen Daten darstellen, sollte die Erfassung möglichst vermieden werden. Dazu ein Beispiel (Best Practice) für den Fall der Aufzeichnung des Nachtigall-Gesangs über eine spezielle App:

> **1. Stufe:**
> Hinweise an die Bürgerforscher, dass keine menschlichen Gespräche oder Äußerungen, auch nicht im Hintergrund, mit aufgezeichnet werden dürfen.
> **2. Stufe:**
> Die Aufzeichnung wird zunächst nur lokal auf dem Smartphone gespeichert. Es erfolgt kein automatischer Upload auf den Server der Institution oder einen anderen Server.

---

[43] Daneben findet nach Auffassung des Bundesgerichtshofs auch das Telemediengesetz (TMG) Anwendung, wobei § 13 Abs. 1 TMG europarechtskonform so auszulegen sei, dass für die dort genannten automatisierten Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen, wie insbesondere Cookies, die von Web-Anwendungen, aber auch Smartphone-Apps eingesetzt werden können, die aktive Einwilligung der betroffenen Person notwendig ist: BGH, Urteil vom 28.05.2020, Az. I ZR 7/16 (Planet49).

3. Stufe:
Lokale technische Möglichkeiten, in der App auf dem Smartphone, dahingehend, dass aus Versehen doch mit erfassten Äußerungen gelöscht werden können, sowie Hinweise hierauf.

4. Stufe:
Hinweis, dass kein Upload solcher Äußerungen auf den Server der Institution erfolgen darf und dass vorher entsprechende Abschnitte gelöscht werden müssen.

5. Stufe:
Auf dem Server der Institution erfolgt eine automatisierte Prüfung (über Mustererkennungsverfahren, zum Beispiel mittels künstlicher Intelligenz), ob menschliche Sprache enthalten ist. Wenn das der Fall ist, werden diese Sequenzen vor dauerhafter Speicherung gelöscht.

6. Stufe:
In Zweifelsfällen der automatisierten Spracherkennung sollte vor dauerhafter Speicherung noch eine menschliche Kontrolle erfolgen.

Somit werden in diesem Beispiel Maßnahmen ergriffen, um zu verhindern, dass personenbezogene Daten Dritter überhaupt schon auf dem Smartphone mittels der App erhoben oder jedenfalls an die dahinterstehende Institution übermittelt werden. **Soweit doch eine solche Verarbeitung personenbezogener Daten** stattfindet ist zwar im Fall der Erhebung für den Bürgerforscher und bei Übermittlung oder gemeinsamer Verantwortung auch für die Institution eine Rechtsgrundlage erforderlich. In der Regel wird angesichts der getroffenen Maßnahmen eine Abwägung im Rahmen von Art. 6 Abs. 1 S. 1 Buchstabe f DSGVO und möglicherweise auch § 27 Abs. 1 BDSG (falls versehentlich Gespräche über die Gesundheit aufgezeichnet würden) zu Gunsten dieser sehr reduzierten Verarbeitung ausgehen. Auch dürfte das Risiko, welches von dieser Verarbeitung für die Rechte und Freiheiten der betroffenen Personen ausgeht, nicht hoch sein, sodass keine formale Datenschutz-Folgenabschätzung nach Art. 35 DSGVO nötig ist. Gleichwohl muss eine **Interessenabwägung** im Rahmen der genannten Rechtsgrundlagen erfolgen und dokumentiert werden, wobei dies bei Art. 6 Abs. 1 S. 1 Buchstabe f DSGVO leichter und kürzer von der Hand geht als bei sensiblen Daten nach § 27 Abs. 1 BDSG.

2. Datenweitergabe durch den Bürgerforscher bzw. die App an eine Institution

Für die weitergehende Auswertung der Forschungsdaten findet bei der Bürgerforschung allerdings häufig eine Datenweitergabe an eine initiierende bzw. koordinierende Institution statt. Die Offenlegung durch **Übermittlung oder Bereitstellung zum Abruf** stellt ebenfalls eine Verarbeitung im Sinne der DSGVO dar. Das heißt, dass die Datenweitergabe auch den Anforderungen der DSGVO unterfällt, sofern hierbei personenbezogene Daten enthalten sind. Es bedarf daher ebenfalls einer Einwilligung des Bürgerforschers und betroffener Personen, sofern das Gesetz keine Erlaubnis vorsieht. Im Hinblick auf Dritte als Beifang kann hier auf die eben bereits zur Datenerhebung durch die Bürgerforscher vorgestellt Abwägungslösung zurückgegriffen werden.

Sofern allerdings die Daten, welche der Bürgerforscher der App über sich selbst verrät, in personenbezogener Form an die Server einer initiierenden/koordinierenden Institution übertragen werden, sollte **bei Installation der App vom Bürgerforscher eine elektronische Einwilligung** eingeholt werden. Dies ist in dieser Konstellation prinzipiell problemlos möglich, was den Rückgriff auf eine reine Abwägungslösung kaum möglich macht oder jedenfalls erheblich erschwert. Die Einwilligung könnte in Kurzform wie folgt aussehen:

Einwilligung

☐ Ich bin damit einverstanden, dass das Museum für Naturkunde, Berlin, die von mir mittels der vorliegenden App hochgeladenen Daten für Zwecke der wissenschaftlichen Forschung wie in den Datenschutzbedingungen näher beschrieben verarbeitet.
Link zu den Datenschutzbedingungen

Dabei ist zu beachten, dass die hier verlinkten Datenschutzbedingungen die Einwilligung als Erklärung des betroffenen Bürgerforschers konkretisieren, also nicht einfach einseitig von der die App herausgebenden Institution geändert werden können. Eine einseitige Änderung wäre bei bloßen Datenschutzhinweisen der Institution grundsätzlich möglich, wobei diese nur genügen, wenn eine andere Rechtsgrundlage als die Einwilligung vorliegt. Jedenfalls solche Datenschutzhinweise müssen nach Art. 13 DSGVO aber zum Abruf über die App in der genannten Konstellation der Datenübermittlung an einen Server bereitgestellt werden.

3. Weiterverarbeitung der Daten durch die initiierende/koordinierende Institution

Auch auf die Weiterverarbeitung finden die bereits oben genannten Voraussetzungen und Grundsätze der DSGVO Anwendungen. Insbesondere die Grundsätze der Pseudonymisierung oder Anonymisierung sind zu beachten.

Soll mit den **Bürgerforschern** als Subjekte der Forschung (aktive Forscher) oder deren Objekte ein weiterer Kontakt gepflegt werden, so kommt insoweit freilich allenfalls die Pseudonymisierung in Betracht, auch welche man bei intensiverem Kontakt mit diesen als Subjekte (aktive Forscher) jedenfalls mit Einwilligung der betroffenen Bürgerforscher auch verzichten kann. Anders sieht dies bei der Erfassung der Daten von **Dritten** als Forschungsobjekte aus, wo zumindest eine frühestmögliche Pseudonymisierung geboten erscheint.

IX. Welche Rechte hat die betroffene Person?

Eine betroffene Person ist jede natürliche Person, welche aus personenbezogenem Daten identifiziert werden kann oder mit Hilfe weiterer Informationen identifizierbar ist. Dieser betroffenen Person stehen gegenüber dem Verantwortlichen Rechte aus den Art. 15 bis 22 DSGVO zu:

1. Auskunftsrecht (Art. 15 DSGVO)

Die betroffene Person kann gegenüber dem Verantwortlichen eine Bestätigung darüber verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden und, falls dies zutreffend ist, Auskunft über diese Daten zu verlangen.

2. Recht auf Berichtigung (Art. 16 DSGVO)

Die betroffene Person hat das Recht, von dem Verantwortlichen die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen.

3. Recht auf Löschung (Art. 17 DSGVO)

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten gelöscht werden, sofern

a) die personenbezogenen Daten **nicht mehr notwendig** sind.

b) die betroffene Person ihre **Einwilligung widerruft** und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt,
c) die betroffene Person gemäß Art. 21 DSGVO einen zu beachtenden **Widerspruch** gegen die Verarbeitung einlegt,
d) die personenbezogenen Daten **unrechtmäßig** verarbeitet wurden,
e) die Löschung zur Erfüllung einer **rechtlichen Verpflichtung** nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich ist, oder
f) die personenbezogenen Daten eines **Kindes** wurden in Bezug auf Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

Keine Anwendung erfährt das Recht auf Vergessen nach Abs. 3 dieser Vorschrift, soweit es rechtmäßige Forschungszwecke gemäß Art. 89 Abs. 1 DSGVO unmöglich machen oder ernsthaft beeinträchtigen würde.[44]

4. Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)

Die betroffene Person das Recht nach Abs. 1 dieser Vorschrift, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn

a) die **Richtigkeit bestritten** wird,
b) die **Verarbeitung unrechtmäßig** ist,
c) der Verantwortliche die personenbezogenen Daten **nicht länger benötigt** oder
d) **Widerspruch** nach Art. 21 Abs. 1 DSGVO eingelegt wurde.

Wurde die Verarbeitung nach Abs. 1 eingeschränkt so dürfen gem. Abs. 2 personenbezogene Daten nur eingeschränkt verarbeitet werden, nämlich

- mit Einwilligung der betroffenen Person oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder
- aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats.

5. Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

Die betroffene Person hat nach Art. 20 Abs. 1 DSGVO das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und **maschinenlesbaren Format** zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern

a) die Verarbeitung auf einer **Einwilligung** oder auf einem **Vertrag** beruht und

b) die Verarbeitung mithilfe **automatisierter Verfahren** erfolgt.

Nach Abs. 2 dieser Vorschrift kann die betroffene Person unter den genannten Voraussetzungen auch die direkte Übertragung ihrer Daten vom ersten auf einen weiteren Verantwortlichen verlangen, soweit dies technisch machbar ist. Im Gegensatz zum Recht auf Auskunft, dass auch durch unstrukturierte Datenkopien zum Beispiel in Papierform erfüllt werden kann, beinhaltet das Recht auf Datenübertragbarkeit die Herausgabe maschinenlesbarer Daten, was die **Weiterverarbeitung deutlich erleichtert**. Dieser

[44] Siehe dazu die Ausnahmen vom Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 Buchstabe e DSGVO oben S. 27 f.

Anspruch kann sich gegen Bürgerforscher und die gegebenenfalls hinter diesen stehenden Institutionen richten, aber auch von Bürgerforschern selbst geltend gemacht werden, sei es gegenüber Dritten zu Gunsten der Bürgerforschung oder gegenüber den koordinierenden Institutionen, gerade wenn die Bürgerforscher der Institution auch Daten über sich selbst per App bereitstellen.

Allgemein besteht dieses Recht nur unter den genannten Bedingungen, wobei die Daten zunächst von der betroffenen Person selbst bereitgestellt worden sein müssen. Als typische Anwendungsfälle für dieses Recht werden daher **soziale Netzwerke** genannt, bei denen die betroffenen Nutzer selbst Beiträge „posten". Dies könnte u. U. für Bürgerforschung zum Kommunikationsverhalten in sozialen Netzwerken genutzt werden, wobei hier Art. 20 Abs. 4 DSGVO zu berücksichtigen sein wird. Diese Vorschrift besagt, dass das Recht auf Datenübertragbarkeit die Rechte und Freiheiten anderer Personen nicht beeinträchtigen darf. Dies könnte dazu führen, dass die mit der betroffenen Person verknüpften Posts anderer Nutzer vom Sozialen Netzwerk möglicherweise nicht herausgegeben oder zuvor anonymisiert werden müssen. Dies müsste wohl in jedem Fall zumindest im Nachgang erfolgen, wenn es sich um nicht-öffentliche Posts Dritter handelt, die die betroffene Person aber nicht nur für ihre privaten Zwecke, sondern für die koordinierte Bürgerforschung mit anderen teilen möchte.

Nicht erfasst sein dürften dagegen zum Beispiel Energieverbrauchsdaten eines Privathaushaltes, da diese nicht von den betroffenen Personen selbst bereitgestellt wurden, sondern vom Energieversorger selbst über die eigenen Stromzähler erfasst wurden.

6. Widerspruchsrecht (Art. 21 DSGVO)

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer **besonderen Situation** ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund öffentlicher oder berechtigter Interessen rechtmäßig (Art. 6 Abs. 1 Buchstabe e oder f DSGVO) ist, Widerspruch einzulegen (Art. 21 Abs. 1 DSGVO). Gleiches gilt für eine Verarbeitung, die wissenschaftlichen oder historischen Forschungszwecken dient, es sei denn, diese ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich (Art. 21 Abs. 6 DSGVO). Im zuletzt genannten Fall könnte aber wiederum das Widerspruchsrecht nach Abs. 1 der Vorschrift greifen.

In jedem Fall muss die betroffene Person hier zunächst Ihre besondere Situation darlegen. Dann muss der Verantwortliche nach Art. 21 Abs. 1 S. 2 DSGVO die **Verarbeitung einstellen, es sei denn,**

- er kann **zwingende schutzwürdige Gründe** für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder
- die Verarbeitung dient der **Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen**.

Diese Rechtsfolgen sind auch auf Art. 21 Abs. 6 DSGVO zu übertragen. Die gegebenenfalls erforderliche Interessenabwägung ist auch in diesem konkreten Kontext zu dokumentieren.

Für den Fall der Einwilligung sei in diesem Zusammenhang darauf hingewiesen, dass die betroffene Person ohnehin über ein unbedingtes Widerrufsrecht verfügt. Eine Abwägung kann hier nur bei der

Frage stattfinden, ob die Daten trotz Widerruf für Zwecke der Nachprüfbarkeit von Forschungsergebnissen noch eine gewisse Zeit aufbewahrt werden dürfen.

7. Beschränkungen der Betroffenenrechte

Weitere Beschränkungen können das Auskunftsrecht (Art. 15 DSGVO), das Recht auf Berichtigung (Art. 16 DSGVO), das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO) und das Widerspruchsrecht (Art. 21 DSGVO) auf Grundlage von Art. 89 Abs. 2 DSGVO durch besondere Vorschriften wie § 27 Abs. 2 BDSG erfahren. Voraussetzung ist, dass diese Rechte voraussichtlich die Verwirklichung der **Forschungszwecke unmöglich machen oder ernsthaft beinträchtigen** und die Beschränkung für die Erfüllung der Forschungszwecke notwendig ist. Zudem soll das Recht auf Auskunft (Art. 15 DSGVO) nach § 27 Abs. 2 S. 2 BDSG nicht bestehen, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

Im Anwendungsbereich der LDSG oder bereichsspezifischer Regelungen ist jeweils zu prüfen, ob die Öffnungsklausel des Art. 89 Abs. 2 DSGVO vom zuständigen Gesetzgeber genutzt wurde. Ein direkter Durchgriff auf diese Norm aus der DSGVO steht den Forschungseinrichtungen nicht zu.

X. Welche Persönlichkeitsrechte sind neben dem Datenschutz zu beachten?

Neben dem Datenschutzrecht werden vorliegend noch zwei im Kontext der Bürgerforschung besonders relevante Persönlichkeitsrechte betrachtet, welche vor allem auf die Betroffenheit einer Person abstellen und nicht – wie das Urheberpersönlichkeitsrecht – primär auf ihre Schöpfungen oder Leistungen. Dabei handelt es sich um das Recht am eigenen Bild und das postmortale Persönlichkeitsrecht.

1. Das Recht am eigenen Bild

> Das **Recht am eigenen Bild** ist eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts und dient dem Schutz der Privatsphäre. Es gibt dem Abgebildeten grundsätzlich die Befugnis, über die **Verbreitung des Bildes selbst zu bestimmen**.

Für das Recht am eigenen Bild und die Veröffentlichung von Personenaufnahmen gibt es eigene Regelungen im **Kunsturhebergesetz (KUG)**.

Allerdings wird das KUG mittlerweile durch die **DSGVO** als höherrangiges und unmittelbar anwendbares Europarecht weitreichend verdrängt, soweit diese anwendbar ist. Die DSGVO findet allerdings keine Anwendung, wenn die Bildnisse keine personenbezogenen Daten enthalten, wie beispielsweise bei Landschaftsaufnahmen. Ebenso fallen Bildaufnahmen, die zu rein privaten Zwecken gemacht werden und ungeordnete analoge Fotografien nicht in den Anwendungsbereich der DSGVO. Bei Letzteren liegt keine automatische Verarbeitung vor. Anders sieht es hingegen bei der mittlerweile weit verbreiteten digitalen Fotografie aus, bei der in den meisten Fällen wohl von einer automatischen Datenverarbeitung durch das Aufnahmegerät selbst und damit von der Anwendbarkeit der DSGVO bei Bildaufnahmen ausgegangen werden muss – soweit die eingangs beschriebene Ausnahme für private und familiäre Zwecke nicht greift.

Zudem gibt **Art. 85 DSGVO** den Mitgliedstaaten durch seine Öffnungsklausel in Abs. 2 zum Zweck der Wissenschaft eigene Regelungsspielräume. Allerdings ist umstritten, ob der nationale Gesetzgeber hierfür eine neue Regelung schaffen muss oder hierfür schon bestehende Regelungen wie die aus dem KUG

ausreichend sind. Dies Bundesregierung geht jedoch davon aus, dass hier eine weitreichende **Öffnungsklausel** vorliegt, weshalb neben dem Einwilligungserfordernis nach § 22 KUG auch die Ausnahmeregelung des § 23 KUG für journalistische, wissenschaftliche oder künstlerische Zwecke unverändert beibehalten werden kann.[45] Vor diesem Hintergrund ist es zumindest vertretbar auch für Zwecke der Bürgerforschung §§ 22, 23 KUG weiter anzuwenden.

Nach **§ 22 KUG** dürfen Bildnisse grundsätzlich nur mit **Einwilligung des Abgebildeten** verbreitet oder öffentlich zur Schau gestellt werden. **Nach dem Tode** des Abgebildeten bedarf es bis zum Ablauf von 10 Jahren der Einwilligung der **Angehörigen** des Abgebildeten. Angehörige im Sinne des KUG sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Abgebildeten und, wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden sind, die Eltern des Abgebildeten.

Prinzipiell steht im KUG ähnlich wie in der DSGVO ein Einwilligungserfordernis an erster Stelle. Dabei kann die Einwilligung auch durch **schlüssiges Handeln** erteilt werden, so zum Beispiel, wenn der Abgebildete für eine Aufnahme „posiert", sofern ihm die Verwendungszwecke klar sind. Sofern der Abgebildete minderjährig ist, bedarf es aber der Einwilligung des gesetzlichen Vertreters (Erziehungsberechtigten). Allerdings kennt auch das KUG Ausnahmen bzw. andere Rechtfertigungsgründe:

Ohne Einwilligung dürfen nach **§ 23 KUG** verbreitet und zur Schau gestellt werden:

1. Bildnisse aus dem **Bereich der Zeitgeschichte** (insbes. Prominente oder wichtige Ereignisse);
2. Bilder, auf denen die **Personen nur als Beiwerk** neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;
3. Bilder von **Versammlungen**, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;
4. Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem **höheren Interesse der Kunst** dient.

Die Befugnis erstreckt sich jedoch nicht auf eine Verbreitung und Schaustellung, durch die ein berechtigtes Interesse des Abgebildeten oder, falls dieser verstorben ist, seiner Angehörigen verletzt wird.

Gemäß § 23 Abs. 2 KUG dürfen also die berechtigten Interessen des Abgebildeten bzw. seiner Angehörigen nicht verletzt werden. Es ist also auch hier, ähnlich wie im Datenschutzrecht nach Art. 6 Abs. 1 S. 1 Buchstabe f DSGVO, eine **Interessenabwägung** erforderlich, wobei auch hier die Interessen an einer bloßen Aufnahme und einer Verarbeitung ausschließlich beim Bürgerforscher und innerhalb der Institutionen der Bürgerforschung eher die Ausschlussinteressen der abgebildeten Person überwiegen können als dies bei der Veröffentlichung der Aufnahme der Fall wäre.

Für die vorgelagerte Aufnahme und Verarbeitung von Personenbildern dürfte bei Vorliegen der übrigen Voraussetzungen jedoch nach wie vor die DSGVO anwendbar sein. Wenn allerdings die Voraussetzung für ein Verbreiten nach dem KUG vorliegen, dürften erst recht diejenigen der DSGVO für die Erhebung und vorgelagerter Verarbeitung erfüllt sein.

---

[45] So die Meinung des Bundesministeriums des Inneren (BMI) nach einer Ausarbeitung des Wissenschaftlichen Dienstes des Bundestages zum „Verhältnis der Datenschutz-Grundverordnung zum Kunsturhebergesetz", 16.05.2018, https://www.bundestag.de/resource/blob/563840/bf59a00573853aabbee2c32ddd01e3cd/WD-3-156-18-pdf-data.pdf. Auch gab der Parlamentarische Staatssekretär im BMI im September 2018 für die Bundesregierung entsprechende Antworten auf schriftliche Fragen von Bundestagsabgeordneten, http://dipbt.bundestag.de/dip21/btd/19/044/1904421.pdf, S. 46-48.

Gerade die Ausnahme nach § 23 Abs. 1 Nr. 1 KUG (Personen und Ereignisse der Zeitgeschichte) sowie Nr. 3 (Teilnahme an Versammlungen) könnten für die **zeitgeschichtliche Bürgerforschung** hilfreich sein und hier sogar eine Veröffentlichung im Rahmen einer Abwägung erlauben. Die Ausnahme gemäß § 23 Abs. 1 Nr. 2 KUG (Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit) könnte beispielsweise im Rahmen von **Naturbeobachtungen bei der Bürgerforschung** eine Rolle spielen.

2. Das postmortale Persönlichkeitsrecht

Die **DSGVO** findet **keine Anwendung** auf personenbezogene **Daten Verstorbener** (vgl. Erwägungsgrund 160 S. 2). Zwar haben die Mitgliedstaaten nach Erwägungsgrund 27 der DSGVO die Möglichkeit, auch Vorschriften zum Schutz Verstorbener zu erlassen, jedoch hat Deutschland von dieser Möglichkeit keinen Gebrauch gemacht, wodurch auch das BDSG und die LDSG insoweit keine Anwendung finden.[46] Wichtige Betroffenenrechte wie das Auskunftsrecht (Art. 15 DSGVO) oder das Widerrufsrecht (Art. 7 Abs. 3 S. 1 DSGVO) gehen also mit dem Tod verloren und stehen auch nicht auf Grundlage des Datenschutzrechts den Angehörigen des Verstorbenen zu. Genauso wenig finden die Pflichten des Verantwortlichen, unter anderem im Hinblick auf den Grundsatz der Zweckbindung (Art. 5 Abs. 1 Buchstabe b DSGVO) oder das Recht auf Vergessenwerden (Art. 17 Abs. 2 DSGVO), weiter Anwendung.

Jedoch sind personenbezogene Daten Verstorbener nicht komplett schutzlos, da sie dem Schutzbereich des sogenannten **postmortalen Persönlichkeitsrechts** unterfallen, welches durch die deutsche Rechtsprechung geschaffen wurde.[47] Grundlage für den Prüfungsmaßstab bildet dabei nach des ausschließlich die Unverletzlichkeit der Menschenwürde (Art. 1 Abs. 1 GG).[48] Diese umfasst zum einen den sozialen Achtungsanspruch eines jeden Menschen, der ihm allein aufgrund seines Menschseins zukommt, zum anderen aber auch den sittlichen, personalen und sozialen Geltungswert, den die Person durch ihre eigene Lebensleistung erworben hat. Letzteres soll das Ansehen der Person in der Gesellschaft schützen.

Das bedeutet für die Bürgerforschung, dass eine Datenverarbeitung, welche den sittlichen, personalen oder sozialen Geltungswert des Verstorbenen untergräbt, verboten ist. Dies kann in der Regel nur bei der **Verbreitung von Daten** der Fall sein, sodass diese einem größeren Empfängerkreis bekannt werden. Eine Erhebung und Verarbeitung nur durch den Bürgerforscher oder innerhalb einer kooperierenden Institution dürfte hierfür noch nicht genügen. Insbesondere im Fall der Veröffentlichung kann dies jedoch anders zu bewerten sein.

Das Schutzbedürfnis Verstorbener schwindet nach Ansicht des Bundesgerichtshofs zudem in dem Maße, in dem die **Erinnerung an den Verstorbenen verblasst** und im Laufe der Zeit auch das Interesse an der Nichtverfälschung des Lebensbildes abnimmt. Eine Verfälschung des Lebensbildes Verstorbener dürfte ohnehin nicht im Interesse der Bürgerforschung liegen. Allerdings kann auch die Verbreitung wahrer, bisher nicht öffentlich bekannter Tatsachen das postmortale Persönlichkeitsrecht beeinträchtigen, wenn erst vor relativ kurzer Zeit Verstorbene betroffen sind, die keine Personen der Zeitgeschichte

---

[46] Entgegen der Empfehlung von Kühling/Martini et al., Die DSGVO und das nationale Recht, 2016, S. 21 ff., https://fah.nrw.de/sites/default/files/asset/document/kuehling_martini_et_al_die_dsgvo_und_das_nationale_recht_2016.pdf.

[47] Daneben sei erwähnt, dass Patientendaten durch die ärztliche Schweigepflicht (§ 203 Abs. 5 StGB) und einige Landeskrankenhausgesetze auch über den Tod des Patienten hinaus geschützt sind, was aber für die Bürgerforschung in der Regel von geringerer Bedeutung ist. Auch die Archivgesetze des Bundes und der Länder kennen Sperrfristen, die meist jedoch nicht vom Zeitpunkt des Todes abhängen, sondern von dem der Aufnahme des Archivguts. Auf die postmortale Wirkung des Rechts am eigenen Bild wurde soeben (S. 36 ff.) bereits hingewiesen.

[48] Vgl. BGH, Urteil vom 20.03.1968 – Az. I ZR 44/66 (Mephisto).

(Prominente) waren. Dies kann gerade dann der Fall sein, wenn über üblicherweise negativ bewertete Eigenschaften und Handlungen berichtet wird. Auch dies kann ausnahmsweise erlaubt sein, erfordert aber eine sehr sorgfältige Abwägung.

Die exakte **Dauer der Schutzbedürftigkeit** lässt sich jedoch nicht abstrakt-generell festlegen. Sie hängt vielmehr von den Umständen des Einzelfalls ab. Dabei wird es neben der Intensität der Beeinträchtigung vor allem auf die Bekanntheit und Bedeutung des geprägten Persönlichkeitsbildes ankommen. Bei dem Maler Emil Nolde ging der Bundesgerichtshof von einer Schutzbedürftigkeit von jedenfalls mehr als 30 Jahren nach dem Tode aus.[49] Das heißt, dass je nach Bedeutung der verstorbenen Person eine Schutzbedürftigkeit von mehreren Jahrzehnten angenommen werden kann. Auch ist in der Rechtsprechung anerkannt, dass in erster Linie vom Verstorbenen zu Lebzeiten berufene Personen und daneben seine nahen Angehörigen als Wahrnehmungsberechtigte für das postmortale Persönlichkeitsrecht anzusehen sind.

Hiervon ist insbesondere die **historische Bürgerforschung** zu Personen betroffen. Dabei lässt sich wohl vertreten, dass postmortale Persönlichkeitsrecht für längst verstorbene Personen des historischen Zeitgeschehens von vor über 100 Jahren bei Verbreitung wahrer Tatsachen wohl kaum mehr verletzt sein wird. Anders sieht es allerdings bei noch nicht so lange verstorbenen Personen aus, deren grundsätzlich schutzwürdiges Abbild im kommunikativen Gedächtnis der Gesellschaft noch nicht verblasst ist und daher eher vor neuen, möglicherweise negativ besetzten Erkenntnissen geschützt ist, was allerdings immer eine Frage der Abwägung im Einzelfall ist.

XI. Welche weiterführenden Quellen gibt es?

Es existiert eine Vielzahl von Literatur, Rechtsprechung und Auslegungshinweisen zur DSGVO, anderen Datenschutzgesetzen und verwandten Persönlichkeitsrechten. Hier kann nur eine Auswahl weiterführender Quellen mit besonderer Bedeutung für die Bürgerforschung in Deutschland wiedergegeben werden:

- *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz):* Kurzpapiere zur Auslegung der DSGVO: https://www.datenschutzkonferenz-online.de/kurzpapiere.html.

- *Rat für Sozial- und Wirtschaftsdaten:* Handreichung Datenschutz; 2. Auflage 2020: https://www.ratswd.de/dl/RatSWD_Output8.6_HandreichungDatenschutz_2.pdf.

- *Europäischer Datenschutzausschuss (bestehend aus Vertretern der Datenschutzaufsichtsbehörden aller Mitgliedstaaten sowie dem Europäischen Datenschutzbeauftragten):* Leitlinien, Empfehlungen, bewährte Verfahren; zum Teil nur in englischer Sprache verfügbar: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de.

[49] BGH, 08.06.1989 - I ZR 135/87 (Emil Nolde). Hier ging es um eine Bildfälschung mit Signatur, was die Übertragbarkeit auf die seriöse Bürgerforschung einschränkt, wenn auch im Hinblick auf den Schutz an sich nicht ausschließt. Wenn unseriöse Bürgerforschung historische Daten zu einer Person fälschen sollte, dürften weitere Teile des Urteils übertragbar sein.