


Forschungsdatenmanagement in der ethnografischen Forschung. Eine praktische Einführung

Sabine Imeri, Martina Klausner und Michaela Rizzolli


Zusammenfassung

Der Umgang mit (digitalen) Forschungsdaten ist in den letzten Jahren vermehrt thematisiert und problematisiert worden. Unter dem Begriff Forschungsdatenmanagement (FDM) werden dabei alle Tätigkeiten im sog. Datenlebenszyklus subsumiert, von wissenschaftlichen Basisoperationen, wie das Ordnen von Material und Dokumentieren von Arbeitsschritten, über die Vorbereitung von Forschungsdaten für die dauerhafte digitale Archivierung, wie etwa die Erstellung von Metadaten, bis hin zur Kontextualisierung von Forschungsprozessen mit dem Ziel der Bereitstellung von Forschungsdaten und Materialien für die weitere Nutzung. Auf allen Ebenen stellen sich neben technischen und praktischen vor allem rechtliche und ethische Fragen. Der Beitrag formuliert Vorschläge zum verantwortungsvollen Umgang mit Daten und Materialien, die von Studierenden und Forschenden selbst erhoben und ausgewertet werden. Er legt einen Schwerpunkt auf Schritte des FDM, die den Forschungsprozess begleiten, und nimmt insbesondere digital vorliegende ethnografische Feldforschungsdaten in den Blick.

Schlagwörter: Forschungsdatenmanagement, Informierte Einwilligung, Datensicherheit, Pseudonymisierung, Datenmanagementplan

Dr. Sabine Imeri, Fachinformationsdienst Sozial- und Kulturanthropologie, Humboldt-Universität zu Berlin sowie Forschungsdatenzentrum Qualiservice, Universität Bremen, Deutschland 

Prof. Dr. Martina Klausner, Institut für Kulturanthropologie und Europäische Ethnologie, Goethe-Universität, Frankfurt am Main, Deutschland 

Dr. Michaela Rizzolli, Forschungsdatenzentrum Qualiservice, Universität Bremen, Deutschland 

Einleitung

In der ethnografischen Forschung ist der Umgang mit digitalen Forschungsdaten und Materialien inzwischen alltägliche Praxis: Forschende führen Interviews mithilfe digitaler Tools, folgen ihren Forschungspartner:innen in den sozialen Medien oder kommunizieren mit Akteur:innen im Feld über Messenger-Dienste. Nach wie vor sind jedoch mögliche Konsequenzen dieser Entwicklung nicht ausreichend thematisiert und problematisiert worden, viele

Fragen, sind (noch) unbeantwortet. Gleichzeitig haben Forschungsförderinstitutionen, wie beispielsweise die Deutsche Forschungsgemeinschaft (DFG), in den letzten Jahren eigene Erwartungen an die Handhabung von (digitalen) Forschungsdaten und Materialien formuliert und eingefordert, dass alle Disziplinen fachspezifisch geeignete Verfahren diskutieren und implementieren. Ein wesentliches Ziel ist dabei, Forschungsdaten und Materialien auch für andere als die ursprünglichen Forschungszwecke dauerhaft zu erhalten und mit möglichst wenig Hürden zugänglich zu machen.

Viele dieser Entwicklungen sind ohne die weitreichende Digitalisierung von Forschungsprozessen kaum denkbar; grundsätzlich betreffen Fragen des Datenmanagements aber auch Material, das nicht genuin digital ist. Der Grundausrichtung des Bandes folgend, soll in diesem Beitrag eine eindeutige Trennung zwischen digital, digitalisiert und analog nicht reproduziert werden. Es geht uns vielmehr darum, der Gegenstandsangemessenheit und Vielfältigkeit methodischer Anwendungen in der ethnografischen Forschung auch mit Blick auf das Forschungsdatenmanagement Rechnung zu tragen. Die in diesem Beitrag beschriebenen Schritte sind entsprechend unabhängig davon einsetzbar, wie welche Daten generiert wurden. Hinsichtlich online erhobener Daten, wie beispielsweise Mitschnitte von Konversationen in Onlinegruppen, sind zudem viele rechtliche Fragen noch ungeklärt. Wann gilt ein Raum im Internet als privat oder öffentlich? Welche Konsequenzen ergeben sich für die Pseudonymisierung bzw. Anonymisierung von Daten? Wir werden uns in diesem Beitrag immer wieder auf Besonderheiten digitaler Forschungsfelder und den aktuellen Stand der Debatten beziehen, beabsichtigen insgesamt aber einen Einblick in grundlegende Schritte des Forschungsdatenmanagements.

Unter dem Begriff Forschungsdatenmanagement (FDM) werden alle materialbezogenen Tätigkeiten im sog. Datenlebenszyklus subsumiert. Dazu zählen basale wissenschaftliche Operationen wie das Ordnen und Verzeichnen von Material oder das Vermeiden von Datenverlust während einer Forschung, aber auch vorbereitende Schritte für die dauerhafte digitale Archivierung von Forschungsdaten, wie etwa die Erstellung von Metadaten, und nicht zuletzt die Dokumentation und Kontextualisierung von Forschungsprozessen, die für die Weiternutzung von Material durch Dritte notwendig sind (vgl. z.B. RatSWD 2023). Auch wenn nicht alle diese Schritte vollständig neu sind, stellen sich auf allen Ebenen technische und technologische, organisatorische und praktische Fragen, mit Blick auf die mögliche Verbreitung und Rekombination digital vorliegender Informationen vor allem aber rechtliche und ethische Fragen mit neuer Dringlichkeit.

Insgesamt wird damit in allen Disziplinen eine stärkere Standardisierung und Formalisierung des FDM angestrebt, die zwar die – notwendige – Professionalisierung im Umgang mit digitalen Forschungsdaten, technischen Werkzeugen und rechtlichen Vorgaben forciert, gleichzeitig aber gerade für die ethnografische Forschung zahlreiche Herausforderungen mit sich bringt: Zum Beispiel sollen Datenerhebungs- und -verarbeitungsschritte am besten vor Beginn einer Forschung in einem sog. Datenmanagementplan festgehalten werden, was mit Blick auf die grundsätzliche Offenheit und Flexibilität ethnografischer Forschung schwierig sein kann. Wenn mit personenbezogenen Daten und Informationen gearbeitet wird, werden wiederum stark formalisierte Anforderungen an die sog. Informierte Einwilligung der betroffenen Personen gestellt. Das lässt sich in vielen Fällen nur schlecht mit situierten, vertrauensbasierten Forschungsbeziehungen vereinbaren. Noch genauer zu bestimmen ist außerdem das Verhältnis von kontextspezifischen und eng an die forschende Person gebundenen ethnografischen Forschungsdaten und den besonderen Anforderungen, die sich ergeben, wenn Daten für die weitere Nutzung durch Dritte zur Verfügung gestellt werden sollen.

Auch wenn es angesichts der Heterogenität der Forschungsfelder und Zugänge ethnografischer Forschung kaum möglich ist, Verfahren und Prozesse zu standardisieren, sind mit Blick auf das entstehende Material wiederkehrende Fragen und Aspekte erkennbar, die sich als Teil von Forschungsdatenmanagement gemeinsam thematisieren lassen. Insofern lässt sich für die ethnografische Forschung zunächst zwar kein allgemeingültiges Verfahren für den Umgang mit Forschungsdaten formulieren, das dann Schritt für Schritt abgearbeitet werden könnte. Die Auseinandersetzung mit zentralen Aspekten und Problemen des FDM kann aber dabei helfen, mit Blick auf die eigene Forschung, den konkreten Fall und das spezifische Material abzuwägen, was sinnvoll und angemessen ist. In diesem Sinne beabsichtigen wir mit diesem Beitrag eine Sensibilisierung für Fragen des verantwortungsvollen Umgangs mit Forschungsdaten und Materialien unter den Bedingungen von Digitalität und formulieren Vorschläge, die im Einzelfall von Studierenden und Forschenden angepasst werden können. Wir legen einen Schwerpunkt auf solche Schritte und Erfordernisse des FDM, die den Arbeitsalltag während einer Forschung begleiten. Fragen der dauerhaften Archivierung und der Nachnutzung hingegen werden am Ende des Textes lediglich angerissen, aber nicht weiter vertieft.

Nach einer kurzen Reflexion zum Datenbegriff in der ethnografischen Forschung und einem knappen Überblick zu den zentralen rechtlichen Grundlagen, greifen wir vier aus unserer Sicht für den Umgang mit ethnografischen Forschungsdaten und Materialien wichtige Aspekte heraus, die wir ausführlicher diskutieren. Wir erläutern jeweils die Grundlagen, gefolgt von praktischen Vorschlägen, die es vor allem Studierenden erleichtern sollen, sich mit Schritten des FDM vertraut zu machen. Ergänzt werden die Vorschläge mit konkreten Beispielen, Tipps und weiterführenden Informationen.

Infobox 1: Allgemeine Informationen zum FDM.

- Die Informationsplattform forschungsdaten.info bietet einen disziplinübergreifenden Einstieg in zahlreiche Themenbereiche (forschungsdaten.info 2023a).
- Das Fachportal Ethnologie ([EVIFA](https://www.evifa.de)) stellt Informationen für die ethnologischen Fächer zu ausgewählten Aspekten bereit. (EVIFA o.J.)

Anmerkungen zum Datenbegriff in der ethnografischen Forschung

Wir wollen zunächst in wenigen Stichworten umreißen, was wir in diesem Text unter Forschungsdaten verstehen, denn im Fachkontext ist keineswegs geklärt, was ‚Forschungsdaten‘ im Rahmen ethnografischer Feldforschung sind, und ob ‚Daten‘ dafür der richtige Begriff ist (Imeri 2018). Unstrittig ist aber, dass Daten nicht mit objektiven Fakten gleichgesetzt werden können, weil sie im sozialen Prozess der Feldforschung hervorgebracht werden und in Feldbeziehungen eingebettet sind. Gesprächspartner:innen gewähren Zugang zu ihrem Alltag, teilen ihr Wissen und persönliche Erlebnisse, berichten von – teils auch intimen oder für sie schwierigen – Erfahrungen und ermöglichen den Forschenden damit einen charakteristischen Lernprozess. Der Aufbau von Forschungsbeziehungen ist ein fortwährender Prozess, der immer wieder ausbalanciert werden muss und der zudem ohne vielfältige Formen der Zustimmung und Kooperation kaum möglich ist. Viele Ethnograf:innen sehen deshalb

Daten und Materialien – unabhängig davon, ob sie digital oder nicht-digital vorliegen – auch als mit Forschungsteilnehmer:innen ko-produziert an. Ethnografische Forschung lässt sich in diesem Sinn nicht einfach als Erhebung oder Sammlung von Daten verstehen, die dann weiterverarbeitet werden. Aus unserer Sicht ist deshalb auch die Unterscheidung von Rohdaten, Primärdaten und Sekundärdaten für die ethnografische Forschung ungeeignet.

Die Kritik an Konzepten ‚objektiver‘ Daten wird flankiert von Ansätzen der Science and Technology Studies, die die formatierenden Effekte digitaler Werkzeuge, Formate und Informationsinfrastrukturen hervorheben. In diesem Verständnis bringen digitale Werkzeuge der Datenerhebung und -verwaltung mit hervor, was als Daten gilt. Sie sind – wie auch ihre nicht-digitalen Vorgänger – als elementarer Bestandteil der ethnografischen Wissensproduktion entsprechend nicht neutral. In diesem Sinne verstehen wir ‚Daten‘ grundlegend als „socio-technical objects“ (Cliggett 2020: 259), als Produkte sozialer Beziehungen und zugleich formatiert durch Medien, Werkzeuge und Infrastrukturen, die im gesamten Forschungsprozess und im gesamten Datenlebenszyklus verwendet werden. Der Umgang mit Forschungsdaten ist überdies geprägt durch disziplinäre „data ideologies“ (Poirier et al. 2020: 213). Damit sind die impliziten wie expliziten disziplinär geprägten Vorannahmen und das Verständnis dessen gemeint, wofür Daten stehen, wie sie genutzt werden können und sollen, und welcher Wert ihnen in einem bestimmten Fachzusammenhang zugeschrieben wird. Poirier et al. folgend, sehen wir die kritische Reflexion fachlicher Daten-Ideologien als eine wesentliche Aufgabe auch bei der Ausgestaltung von Forschungsdatenmanagementprozessen an.

Die Heterogenität der Begriffsverwendungen und ihre Kritik im Blick, greifen wir hier gleichwohl auf eine ebenso allgemeine wie umfassende Definition von ‚Forschungsdaten‘ zurück, die alle Formen wissenschaftlicher Wissensproduktion umfasst: Forschungsdaten sind demnach

„alle digital vorliegenden Daten, die während des Forschungsprozesses entstehen, [...] z.B. durch ein Experiment in den Naturwissenschaften, eine dokumentierte Beobachtung in einer Kulturwissenschaft oder eine empirische Studie in den Sozialwissenschaften [...]. Digitale Forschungsdaten entstehen in allen Wissenschaftsdisziplinen und unter Anwendung verschiedener Methoden, abhängig von der Forschungsfrage.“ (Kindling & Schirnbacher 2013: 130)

In diesem Sinne entstehen in kaum standardisierbaren Situationen der Beobachtung, des Fragens und Erzählens, aus informellen Gesprächen oder Interviews ethnografische Forschungsdaten und Materialien, die in heterogenen Formen und (technischen) Formaten vorliegen und meist in komplexer Weise aufeinander bezogen sind, wie z.B. Beobachtungsprotokolle und Feldnotizen, Interviewtranskripte, Fotos, Videoaufnahmen, aber auch Konvolute von Posts, Chatverläufen und Blogbeiträgen. Im Text selbst verwenden wir vor allem den Begriff Forschungsdaten, der in diesem umfassenden Verständnis auch verwandte Begriffe wie Forschungsmaterialien, Dokumente, Quellen oder Informationen einzuschließen vermag.

Infobox 2: Fachspezifische Empfehlungen und Positionen zum Umgang mit Forschungsdaten in den ethnologischen Fächern.

- [Handreichung zum Umgang mit Forschungsdaten](#) (DFG-Fachkollegium 106 2020).
- [Positionspapier zur Archivierung, Bereitstellung und Nachnutzung von Forschungsdaten](#) (DGEKW 2018).
- [Positionspapier zum Umgang mit ethnologischen Forschungsdaten](#) (DGSKA 2019).
- [Statement on Data Management in Ethnology and Folklore](#) (SIEF 2019).
- [Statement on Data Governance in Ethnographic Projects](#) (EASA 2018).

Ethnografische Daten im Schnittfeld von Recht und Ethik

Die Verbreitungsmöglichkeiten und vor allem die Rekombinierbarkeit digital vorliegender Daten haben zu einer erneuten Auseinandersetzung mit den rechtlichen Rahmungen des Umgangs mit Forschungsdaten geführt. In diesem Zusammenhang sind Rechtsvorschriften erstmals ausführlicher dargelegt und rechtliche Grenzen und Einschränkungen im Umgang mit Forschungsdaten beschrieben worden (vgl. Baumann et al. 2021). Es kommt hier zunächst darauf an, die einschlägigen Vorschriften und Möglichkeiten zu kennen, um dann im Kontext der eigenen Forschung einzuschätzen und abzuwägen, wie der verantwortungsvolle Umgang mit konkretem Material sichergestellt werden kann.

In der ethnografischen Feldforschung sind insbesondere Fragen des Daten- und Persönlichkeitsschutzes relevant, weil hier in oft sehr überschaubaren sozialen Feldern nicht nur Material entsteht, das personenbezogene Informationen, sondern regelmäßig auch sog. besondere Kategorien personenbezogener Daten enthält, wie etwa Hinweise auf politische Haltungen, sexuelle Orientierung, religiöse Zugehörigkeit oder Krankheiten. Die Erstellung und Verarbeitung personenbezogener Daten ist dann rechtskonform möglich, wenn eine informierte Einwilligung der betroffenen Person eingeholt worden ist und/oder wenn spezifische Maßnahmen zum Schutz dieser Daten ergriffen werden, beispielsweise durch eine Pseudonymisierung bzw. Anonymisierung der Namen und ggf. weiterer relevanter Parameter. Dabei müssen alle Verarbeitungsschritte – das meint z.B. die Speicherung, Transkriptionen oder eben die Pseudonymisierung bzw. Anonymisierung – nachvollziehbar in einem „Verzeichnis für Verarbeitungstätigkeiten“ (Art. 30 DSGVO), wie es im Datenschutzgesetz heißt, dokumentiert werden. Zu den möglichen Schutzmaßnahmen zählen auch technische und organisatorische Vorkehrungen, die der Datensicherheit dienen und den nicht gewollten Zugriff auf (personenbezogene) Informationen verhindern sollen, wie insbesondere die Vergabe von Passwörtern, die Nutzung von Verschlüsselungstechniken und sicheren Speicherorten, aber auch Regelungen zur Löschung von Daten. Insofern verhindern Datenschutzgesetze nicht einfach die Arbeit mit personenbezogenen Informationen, sondern legen die Bedingungen fest, unter denen diese Arbeit möglich ist.

Maßgeblich sind die Datenschutzgrundverordnung (DSGVO) der EU von 2018 sowie die darauf aufbauenden nationalen Bundes- und Landesdatenschutzgesetze. Die hier formulierten Regelungen beziehen sich auf das Recht jeder Person, über die Preisgabe und Verwendung von Informationen, die sie betreffen, selbst zu bestimmen. Mögliche Belange und Interessen von Gruppen oder Communities hingegen werden aktuell vom Gesetz nicht erfasst

(vgl. Imeri & Rizzolli 2021: 11). In diesem Sinne sind die Datenschutzgesetze nur dann relevant, wenn sich im Material tatsächlich Informationen über einzelne, identifizierbare Personen befinden.

Ethisch begründete Überlegungen berühren häufig ähnliche Fragen, sind aber rechtlichen Regelungen und Absicherungen nicht deckungsgleich und haben „in erster Linie etwas mit sozialer Verantwortung zu tun“ (Unger 2014: 32). Das gilt auch, wenn sich Beobachtungen auf identifizierbare Gruppen von Menschen mit gemeinsamen Merkmalen beziehen, wie beispielsweise spezifische Nachbarschaften, aktivistische Gruppen oder kleine Religionsgemeinschaften, auch wenn einzelne Personen im Material nicht erkennbar sind. Unabhängig davon muss – dem ethischen Prinzip des „do no harm“ folgend – der Umgang mit dem Material so gestaltet werden, dass Forschungsteilnehmer:innen oder Dritten kein Schaden durch die Verarbeitung von Daten entsteht bzw. dass Risiken minimiert werden. In manchen Fällen kann die Angemessenheit von Schutzmaßnahmen bzw. die Abwägung möglicher Risiken – und damit auch, welche Fragen und Aspekte in einem konkreten Feld, einer konkreten Situation überhaupt ethisch relevant sind – im Sinne einer kollektiven ethischen Praxis nur mit den Akteur:innen im Feld ausgehandelt werden. Die Verantwortung liegt letztlich bei den Forschenden. Fragenkataloge und Checklisten sind daher nicht ausreichend, um ethische Fragen abschließend zu entscheiden. Die Auseinandersetzung mit Forschungsethik soll vielmehr als reflexiver Prozess den gesamten Forschungsprozess begleiten und am besten auch im Austausch mit anderen Forscher:innen stattfinden.

Insgesamt gilt für ethnografische Forschung, dass ethische Fragen oftmals über rechtlich geforderte Datenschutzmaßnahmen hinausgreifen – oder im Rahmen von Datenschutzmaßnahmen etwa bei der Informierten Einwilligung entstehen (siehe unten) – und Forschende auch auf fachspezifische Anforderungen reagieren müssen. Ethnografisch Forschende sind in diesem Sinne aufgefordert, nicht nur ihre eigene Rolle und die Beziehung zu den Forschungsteilnehmer:innen, sondern auch ihren eigenen Umgang mit Daten und Material kontinuierlich und kritisch zu reflektieren.

Definitionsbox 1: Personenbezogene Daten. Personenbezogene Daten sind Angaben, „die irgendeine Beziehung zu einer natürlichen Person herstellen, also der Identifizierung und Beschreibung der betreffenden Person dienen, wie dies im Einzelfall etwa bei dem Namen, der Anschrift, dem Familienstand, dem Geburtsdatum, der Staatsangehörigkeit, dem Erscheinungsbild, der Leistungen, dem Arbeitsverhalten, dem Gesundheitszustand oder religiösen oder weltanschaulichen Überzeugungen der Fall sein kann.“ (Baumann et al. 2021: 172)

Besonders schützenswerte Kategorien personenbezogener Daten sind „Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie [...] genetische[n] Daten, biometrische[n] Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person [...].“ (Art. 9, Absatz 1 DSGVO)

Eine [Übersicht zu den relevanten Datenschutzgesetzen des Bundes und der Länder](#) findet sich auf den Seiten des Virtuellen Datenschutzbüros, das von den Datenschutzbeauftragten der Länder und Partnerinstitutionen verantwortet wird (Virtuelles Datenschutzbüro o.J.).

Konkrete Schritte im FDM

Im Folgenden stellen wir vier Hilfsmittel und mögliche Schritte ausführlicher vor, die für einen ethisch angemessenen Umgang mit digitalen Forschungsdaten und/oder mit Blick auf den skizzierten rechtlichen Rahmen wesentlich sind: Erstens den Datenmanagementplan, der dabei unterstützt, den Umgang mit Forschungsdaten während des gesamten Forschungsprozesses (und darüber hinaus) zu planen und zu dokumentieren; zweitens die informierte Einwilligung (*informed consent*), die als ein Instrument des Datenschutzrechts auch mit zentralen ethischen Fragen im ethnografischen Forschungsprozess verknüpft ist. Drittens schlagen wir Techniken und Werkzeuge vor, die vor allem den sicheren Umgang mit Daten unterstützen, und erläutern viertens Möglichkeiten, Forschungsdaten zu pseudonymisieren bzw. zu anonymisieren. Nur anschnelden werden wir am Ende Fragen rund um die Archivierung von Forschungsdaten. Einführende und praktische Schritte werden jeweils ergänzt durch eine kritische Reflexion zu den „unerwünschten Nebeneffekten“ und Passungsproblemen einer potenziellen Standardisierung und Formalisierung (und Managementlogik) für ethnografische Forschung. Wesentliche Aspekte können hier nur beispielhaft und eher allgemein thematisiert werden. In der ethnografischen Feldforschung entscheidend sind aber die jeweils feldspezifische Reflexion und die Anpassung allgemeiner Vorgaben und Empfehlungen an den Einzelfall, die spezifischen Bedingungen und Erfordernisse eines Feldes sowie konkreter Settings.

I: Organisieren und Dokumentieren – der Datenmanagementplan

Ein Datenmanagementplan (DMP) ist ein Werkzeug, mit dem der Umgang mit Daten und Material im gesamten Forschungsprozess systematisch reflektiert und dokumentiert werden kann – von der Planung eines Projekts über die Materialerstellung und die Analyse bis hin zur möglichen Archivierung am Projektende und der Aufbereitung für die Nachnutzung. Für Forschende kann ein DMP Anlass sein, sich frühzeitig im Projektverlauf auch mit der Frage auseinanderzusetzen, was mit Daten und Material nach Abschluss des Forschungsprojekts passieren soll. Eine erste Version des DMP wird im Idealfall bereits erstellt, bevor die eigentliche Forschung beginnt. Für ethnografische Forschung bzw. allgemein für qualitative Forschung stellt die zielgerichtete Planung des Umgangs mit Forschungsdaten vorab eine gewisse Herausforderung dar, weil eine grundlegende Offenheit des Forschungsprozesses wesentlich ist. Unabhängig davon schafft aber ein regelmäßig aktualisierter DMP Übersicht in einem zentralen Dokument. Gerade in der ethnografischen Forschung, die oft sehr heterogenes Material hervorbringt, kann das nützlich sein. Beispielsweise lassen sich damit Formate, Orte der Speicherung, Backup-Verfahren, Richtlinien zur Benennung von Dateien aber auch Zuständigkeiten festhalten oder notwendige Ressourcen für die datenschutzkonforme Verarbeitung von Forschungsdaten einplanen. Für die inhaltliche Gestaltung eines DMP gibt es keine verbindlichen Vorgaben, vielmehr liegen allgemeine Richtlinien und Empfehlungen für Fachdisziplinen oder Wissenschaftsbereiche vor (siehe Infobox 3). Wie komplex ein DMP wird, hängt maßgeblich vom konkreten Forschungsprojekt und den Rahmenbedingungen ab: Werden sehr unterschiedliche Datentypen erzeugt? Sind mehrere Forschende beteiligt und müssen daher unterschiedliche Rollen und Zugriffe auf die Daten festgelegt werden? Sind Forschungspartner:innen beteiligt, deren Situation besondere Formen der Einwilligung erfordert, wie zum Beispiel Minderjährige oder Menschen, die das Lesen und Schreiben nicht ausreichend beherrschen? Werden Forschungsdaten generiert,

die über die einzelne Forschung hinaus in einem Forschungsdatenzentrum oder Repository zugänglich gemacht werden sollen? Gibt es Vorgaben von Fördergebern, die berücksichtigt werden müssen?

Forschungsprojekte, die über einen Zeitraum von mehreren Jahren eine große Menge an ethnografischen Daten produzieren, die zudem nach Projektende einer wissenschaftlichen Nachnutzung zugänglich gemacht werden sollen, werden z.B. einen differenzierteren Datenmanagementplan benötigen als studentische Forschungen, die mit kleineren Datenmengen arbeiten, die in der Regel nicht zugänglich gemacht werden. Inzwischen werden an den meisten Universitäten FDM-Services und Beratungen für Forschungsprojekte angeboten, auch liegen zahlreiche Leitlinien, Empfehlungen und Vorgaben von Dritten (Universitäten, Förderinstitutionen, Fachgesellschaften, kooperierenden Einrichtungen etc.) vor, die bei der Planung des Umgangs mit Forschungsdaten ggf. zu berücksichtigen sind (siehe Infobox 2). Einige Forschungsförderer verlangen zudem die Erstellung eines Datenmanagementplans als Bestandteil des Förderantrags oder während der ersten Projektphase (so etwa im Programm „Horizon Europe“ der Europäischen Kommission).

Im Folgenden konzentrieren wir uns daher auf Vorschläge für – seltener adressierte – studentische Forschungen, die sich aber auch für umfangreichere Vorhaben ausbauen lassen. Zunächst ist der DMP nicht als ein statisches, sondern als ein lebendes Dokument (*living document*) gedacht, das sich vor dem Hintergrund der methodischen Offenheit immer wieder an die Bedürfnisse der Forschung anpassen lässt. Ein DMP orientiert sich in der Regel am Datenlebenszyklus, der modellhaft einen unspezifischen Forschungsprozess abbildet und von der Datenerhebung über die Datenaufbereitung und Auswertung bis hin zur Archivierung und Bereitstellung von Material für die Nachnutzung alle möglichen Schritte des Datenmanagements adressiert (vgl. z.B. RatSWD 2023: 8). Um diesen Lebenszyklus nachzuerfolgen, reichen gerade für studentische Projekte in der Regel einfache Übersichtstabellen aus, in denen systematisch und chronologisch die Materialerhebung und -verarbeitung dokumentiert werden. Ziel ist es nicht, den Forschungsprozess an einen Plan anzupassen, sondern vielmehr den DMP zu nutzen, um die eigene Forschung zu organisieren.

Diese Übersichtstabelle (siehe Abb. 1) sollte zunächst zentrale Informationen über einzelne Daten bzw. Dateien enthalten – zuallererst den Dateinamen (siehe auch den Abschnitt zur Dateibenennung). Wichtig sind außerdem Informationen zur jeweiligen Materialart: Beinhaltet die betreffende Datei eine Interviewaufzeichnung, eine Gesprächsnotiz, eine Videoaufnahme, ein Beobachtungsprotokoll etc.? Wann wurde das Material erstellt? Bei mehreren beteiligten Forscher:innen: Wer hat es erstellt? Ergänzend kann der Ort der Erstellung oder auch die Dauer eines Interviews oder einer Beobachtung dokumentiert werden.

Zudem sollten in der Tabelle die verschiedenen Schritte der Verarbeitung, ergänzt um den jeweiligen Speicherort, dokumentiert werden:

- In welcher Form wurde das Material erhoben und festgehalten? (z.B.: „handschriftliche Feldnotiz“ oder: „Audioaufnahme mit Aufnahmegerät“)
- Welche weiteren Bearbeitungsschritte wurden getätigt? (z.B.: „Notiz wurde am 27.3.2021 digitalisiert und im Forschungsdatenordner in der Instituts-Cloud gespeichert“ oder: „Aufnahme wurde am 27.3.2021 transkribiert, Transkript in der Instituts-Cloud gespeichert, Audioaufnahme von Aufnahmegerät und Laptop gelöscht am 29.3.2021“) Dies kann noch weiter ergänzt werden, beispielsweise wenn Daten mit einer Analysesoftware bearbeitet wurden oder mit den Forschungspartner:innen eine Vorlage und Freigabe der Daten vereinbart wurde.

Datei-Name/ID	Quelle (Typ, Datum der Erstellung, Ort, Dauer)	Verarbeitungsstand und Speicherort mit jeweiligem Datum			Rechtlklärung		Sonstige Anmerkungen
FN_2021_06_21	Feldnotiz vom Sommerfest im Jugendzentrum am 21.6.2021	Handschriftliche Notizen	Digitalisiert am 24.6.2021 und in Instituts-Cloud hochgeladen	Keine personenbezogenen Daten dokumentiert	Nicht notwendig; aber Leitung des Jugendzentrums war informiert		
Foto_2021_06_21	Foto vom Sommerfest	Handy-Aufnahme, gelöscht am 24.6.2021	in Instituts-Cloud hochgeladen am 24.6.2021		Keine einzelnen Personen fotografiert, unspezifisch in die Gruppe		
IV_Jugendliche1	Interviewaufnahme, 27.3.2021, Jugendzentrum, 57 Minuten Länge	Audiodatei von Aufnahmegerät auf Laptop transferiert am 28.3.2021; Datei im Laptop nach Transkription gelöscht am 5.4.2021	Transkribiert, gespeichert in der Instituts-Cloud am 5.4.2021	am 5.4.2021 pseudonymisiert, in die Instituts-Cloud geladen, nicht-pseudonymisiertes Transkript gelöscht, in Schlüsseldatei dokumentiert, Schlüsseldatei an anderem Ort gespeichert und mit Passwort versehen	Informierte Einverständniserklärung liegt vor (getrennt von den Daten und lokal gesichert), Zusatz für Eltern formuliert (opt-out), Freigabe für Seminkontext, BA-Arbeit und mögliche Veröffentlichung erteilt	Keine Rechte Dritter involviert	Hintergrundgeräusche ab Minute 13 sehr laut; nach Gedächtnis ergänzt; Memo zum Interview erstellt, ebenfalls in der Instituts-Cloud gespeichert

Abbildung 1: Beispiel für eine Übersichtstabelle

- Was ist der Stand der Pseudonymisierung des jeweiligen Materials? (z.B.: „Feldnotizen enthalten keine personenbezogenen Daten, deshalb keine Pseudonymisierung notwendig“ oder: „Interviewtranskript wurde am 14.4.2021 pseudonymisiert und in der Instituts-Cloud gespeichert, nicht-pseudonymisiertes Transkript wurde am 14.4.2021 gelöscht; Schlüsseldatei wurde entsprechend ergänzt“)

Es empfiehlt sich, die Rechteklärung in einem eigenen Abschnitt zu dokumentieren. Die Rechteklärung im Bereich Datenschutz dokumentiert die Form der Einverständniserklärung und welche Besonderheiten hier gegebenenfalls vereinbart wurden (z.B. „Informierte Einverständniserklärung liegt vor, Zusatz für Eltern mit opt-out-Möglichkeit formuliert, Freigabe für Seminarkontext, BA-Arbeit und mögliche Veröffentlichung erteilt“). Zu berücksichtigen ist dabei auch, inwiefern Rechte Dritter betroffen sind – beispielsweise, wenn Gesprächspartner:innen immer wieder namentlich auf konkrete Personen Bezug nehmen, die dann ebenfalls pseudonymisiert bzw. anonymisiert werden müssen. Sofern Urheberrechte zu beachten sind – etwa, wenn in Publikationen oder auf Webseiten Bilder verwendet werden sollen, die die Forscherin nicht selbst erstellt hat – sollte auch dazu eine Notiz hinterlegt werden. Als hilfreich hat sich außerdem erwiesen, eine Kategorie für weitere Anmerkungen zu erstellen, in der beispielsweise Besonderheiten der technischen Qualität der Daten oder der Erhebungssituation genannt werden können. Sollen Daten für eine weitere Verwendung durch andere Forschende zur Verfügung gestellt werden, kann eine eigene Kategorie ergänzt werden, die Details zur Archivierung und zum Zugangsmanagement enthält.

Planung bedeutet also, insbesondere den Prozess der Verarbeitung von Material so weit wie möglich zu antizipieren und weitere konkrete Schritte so zu entwickeln bzw. Vorkehrungen so zu treffen, dass die datenschutzkonforme Handhabung der Daten damit abgedeckt ist. Darüber hinaus unterstützt der DMP dabei, den Überblick über die Umsetzung zu behalten und Nachvollziehbarkeit zu gewährleisten – auch nach Beendigung eines Projekts.

Infobox 3: Nützliche Links und Hilfen für die Erstellung eines DMP in Forschungsprojekten.

- [Checkliste zur Erstellung eines Datenmanagementplans in der empirischen Bildungsforschung](#) (VerbundFDB 2015).
- [Adapt your Data Management Plan. A list of Data Management Questions based on the Expert Tour Guide on Data Management](#) (CESSDA 2019).
- [Webseite](#) mit DMP-Musterplänen für verschiedene Forschungsförderer und Beispielen aus der Praxis (Humboldt-Universität zu Berlin 2023).
- [Der Datenmanagementplan. Eine Wegbeschreibung für Daten](#) (forschungsdaten.info 2023b). Neben allgemeinen Informationen bietet die Seite eine Übersicht zu kostenfreien DMP-Tools im Web, die bei der Erstellung von Datenmanagementplänen unterstützen können.

II: Zustimmung einholen – Die Informierte Einwilligung

Im Rahmen der Datenschutzgrundverordnung (DSGVO) kommt der Informierten Einwilligung eine besondere Bedeutung zu. In wissenschaftlichen Forschungen wird sie immer dann

benötigt, wenn entstehendes Forschungsmaterial personenbezogene Informationen beinhaltet. Sie erlaubt deren weitere Verarbeitung für einen oder mehrere bestimmte Zwecke – hier den konkreten Forschungszweck, vielleicht eine Publikation sowie ggf. auch die dauerhafte Archivierung in einem Forschungsdatenzentrum für mögliche Nachnutzungen. In Einzelfällen ist die rechtmäßige Verarbeitung personenbezogener Daten zu Forschungszwecken auch ohne Einwilligung möglich, z.B. im Rahmen der sog. Interessensabwägung (Art. 6 Abs. 1 lit. f. DSGVO).

Einwilligung bedeutet im Datenschutzrecht, dass betroffene Personen – z.B. Gesprächspartner:innen oder Personen, mit denen man im Rahmen einer teilnehmenden Beobachtung so interagiert, dass sie im Material erkennbar werden – freiwillig und in „informierter Weise“ (Art. 4 Nr. 11 DSGVO) zustimmen, sich in einer bestimmten Form an einer Forschung zu beteiligen. Auch wenn Forschungsdaten archiviert und über das konkrete Forschungsvorhaben hinaus genutzt werden sollen, müssen Gesprächspartner:innen ihre Zustimmung geben. „Informiert“ bedeutet, dass ihnen transparent gemacht werden muss, zu welchem Zweck und wie die sie betreffenden Informationen verarbeitet werden.

Die Einwilligung kann verweigert oder jederzeit ohne Angabe von Gründen zurückgezogen werden (Art. 7 Nr. 3 DSGVO). Ein Widerruf bezieht sich dann jedoch auf die zukünftige Nutzung der Daten und nicht auf bereits erfolgte Verarbeitungen, z.B. in einer Publikation. Daten, die ursprünglich personenbezogen waren, zwischenzeitlich jedoch anonymisiert wurden, bleiben vom Widerruf unberührt und können aus rechtlicher Sicht weiter genutzt werden. Forschende müssen dafür Sorge tragen, dass die Betroffenen bei Einholung der Einwilligung darüber ausreichend informiert wurden (RatSWD 2020: 22). Im Idealfall benennen Forschende bereits zum Zeitpunkt der Datenerhebung möglichst genau, wofür die Daten verwendet werden sollen (z.B. für eine Hausarbeit, die nicht veröffentlicht wird, oder für eine Publikation), damit die betreffenden Personen dem Zweck der Verarbeitung zustimmen oder widersprechen können.

Weil es hierbei um die rechtliche Absicherung und damit um die Zuweisung von Verantwortung im Konfliktfall geht, ist die Informierte Einwilligung hochgradig formalisiert – und damit ein Instrument, das nicht immer zum Vorgehen in der Feldforschung passt. Während in der Regel empfohlen wird, ein ausführlich erläuterndes Formular mit Verweisen auf die entsprechenden Paragraphen des Datenschutzrechts bereits vor einer Forschung unterschreiben zu lassen, wird Einverständnis in der ethnografischen Feldforschung prozesshaft hergestellt und muss immer wieder aktiv stabilisiert und aktualisiert werden. Denn dass Gesprächspartner:innen und andere Akteur:innen mit der Teilnahme an der Forschung einverstanden sind, ist keine rein rechtliche, sondern auch eine zentrale ethische Anforderung an die Feldforschung, die keineswegs neu ist. Forschungsteilnehmer:innen zu informieren bedeutet, dass die Forscher:in sich selbst als forschende Person vorstellt und in verständlicher Sprache ihr Anliegen genauso erläutert wie ihr Vorgehen sowie auf mögliche Risiken hinweist – und dabei auch nachvollziehbar erklärt, was mit Informationen, Daten und Materialien passieren wird. Informiertheit herzustellen, umfasst somit weit mehr als das reine Ausfüllen eines Formulars und stellt aus unserer Sicht den wesentlichen Aspekt der Informierten Einwilligung dar.

Eine Informierte Einwilligung einzuholen, heißt in diesem Sinne, nicht nur die Informationssouveränität, sondern auch Autonomie und Selbstbestimmung einer Person zu respektieren. Insofern ist sie durchaus ein Instrument, das über die datenschutzrechtliche Dimension hinaus auch die Reflexion der eigenen Rolle und ethisch angemessenes Vorgehen im

Feld unterstützen kann – auch wenn sie kaum alle möglichen auftauchenden ethischen Fragen beantworten wird. In diesem Sinne kann eine einmal gegebene Einwilligung die Forscher:in nicht von der darüber hinaus reichenden ethischen Verantwortung – auch für den Umgang mit Forschungsdaten – befreien. Und auch wenn es eine Einverständniserklärung gibt, sollte jeweils geprüft werden, ob Informationen auch tatsächlich verwendet werden sollten bzw. in welcher Form das vertretbar geschehen kann. Dabei gilt es auch, das Einverständnis unter dem Aspekt von Machtasymmetrien zu reflektieren. So ist in der Forschungsarbeit mit vulnerablen Gruppen, z.B. im Kontext von Migration, Gewalt oder politischem Aktivismus, aber auch bei Forschungen mit Minderjährigen, die Freiwilligkeit der Erklärung besonders deutlich zu machen, weil die Betroffenen sonst leicht annehmen könnten, dass die Einwilligung erteilt werden müsse bzw. die Verweigerung einer Einwilligung mit Nachteilen verbunden wäre.

Beispielbox 1: Beispiel aus der Forschung von Jonathan Greenleaf (siehe auch den Band [KA Notizen 84](#)). Jonathan hat in seiner Forschung zu inklusiven Museumsführungen unter Beteiligung von Menschen mit Beeinträchtigungen mit unterschiedlichen Akteur:innen Interviews und Teilnehmende Beobachtungen durchgeführt. Der Hauptakteur seiner Forschung war Jannik (Name pseudonymisiert), der unter anderem Lernschwierigkeiten hat. Um sicherzustellen, dass Jannik die Einwilligungserklärung und die Informationen versteht, hat Jonathan die Einwilligungserklärung in Leichter Sprache erstellt. Andere Akteur:innen, die Jonathan interviewt hat, waren wiederum aufgrund ihrer offiziellen Rolle nicht pseudonymisierbar. Diese Einschränkung hat Jonathan ebenfalls in der entsprechenden Einverständniserklärung erläutert. Grundsätzlich gilt, dass die Einwilligungserklärungen an die jeweilige Forschungssituation angepasst werden und selbst im Rahmen ein und derselben Forschung unterschiedlich gestaltet werden müssen.

Zu klären ist also zunächst, ob in einer Forschungssituation eine Einwilligung benötigt wird. Das ist nicht immer eindeutig: Während Interviews typischerweise eine Einwilligung erfordern, ist das insbesondere in Szenarien der Teilnehmenden Beobachtung oft weniger klar. Informelle Gespräche z.B. bei mehr oder weniger öffentlichen Anlässen oder forschungsrelevante Mitteilungen im Rahmen zufälliger Begegnungen lassen eine ausführliche Information über die Tätigkeiten der Forscher:in in der Regel gar nicht zu. Maren Heibges et al. schlagen in diesem Zusammenhang vor, solche Szenarien entlang von Erwartungen an die Privatsphäre zu skalieren, um zu beurteilen, ob und inwieweit eine Zustimmung erforderlich ist: Je mehr Privatsphäre in einer Situation – in einer therapeutischen Sitzung z.B. eher als auf einem Wochenmarkt – gewünscht wird bzw. erwartet werden kann, desto wichtiger wird die Informierte Einwilligung (Heibges et al. 2019).

Dies gilt ebenso bei Forschungen im Internet oder in und mit digitalen Diensten. Auch hier muss situationsabhängig abgewogen werden, ob Menschen von einem (semi-)privaten Raum ausgehen oder sich in der Öffentlichkeit wähen. Zwar gibt es im Datenschutzrecht einige Hinweise, wie Forschende mit Daten arbeiten können, die von Personen online selbst veröffentlicht werden und allgemein zugänglich sind, gleichwohl ist dabei vieles nach wie vor im Unklaren. Generell gilt es hier ebenfalls, den jeweiligen Kontext und mögliche Erwartungen an die Privatsphäre der Betroffenen zu beachten. Wenn bspw. eine Person in einem frei zugänglichen Forum oder einem Blog personenbezogene Informationen über sich preisgibt, ist dies anders zu bewerten als wenn das in einem über eine Mitgliedschaft regulierten

Raum geschieht. Golla et al. (2018) schlagen deshalb vor, zuerst einmal zwischen offenen und geschlossenen Sozialen Medien zu unterscheiden. Oftmals verfügen Soziale Medien, wie bspw. Facebook, über beides – Bereiche, die offen und allen zugänglich sind, die sich registriert haben, und solche, die nur ausgewählten Personen zugänglich sind. Allerdings sind hier die Grenzen oftmals fließend und es stellt sich die Frage, „ab welcher Zugangsbarriere sich Informationen in Sozialen Netzwerken nicht mehr als öffentlich ansehen lassen“ (ebd.: 97). Während dies aus juristischer Perspektive durch eine Prüfung der Zugangsregeln in Geschäftsbedingungen und der damit verbundenen Einverständniserklärungen differenziert werden kann, bleibt in der ethnografischen Forschung die ethische Verpflichtung bestehen, die Schutzinteressen der Betroffenen und die Interessen der Forschung sorgfältig abzuwägen. Entscheidend ist, dass nicht alles, was an Daten im Internet und darüber hinaus zugänglich ist, auch ohne weitere Information und Einwilligung für die Forschung herangezogen werden kann.

Zeitpunkt der Einwilligung

Die Einwilligung sollte der Erhebung und Verarbeitung personenbezogener Informationen vorausgehen und nicht erst rückwirkend eingeholt werden. Es kann ausreichen, die Einwilligung der betroffenen Personen einmalig einzuholen – wenn sich die Zwecke der Datenverarbeitung ändern, muss jedoch eine neue ausdrückliche Einwilligung eingeholt werden.

Der Zweck muss so konkret angegeben werden, dass die betroffene Person versteht, wofür es in der Forschung geht und was mit den Daten passiert. Wird die Einwilligung zu unterschiedlichen Zwecken benötigt, kann es unter Umständen sinnvoll sein, verschiedene Zeitpunkte zu wählen und zweckgebundene Formulare aufzusetzen (z.B. eine Einwilligung zur Teilnahme an einer Forschung und eine weitere Einwilligung zur Weitergabe, Archivierung und Nachnutzung). Zudem wird mit diesem Vorgehen verhindert, dass die Informierte Einwilligung gerade zu Beginn der Forschung mit vielfältigen Informationen überfrachtet wird. Von einer allgemeineren breiten Einwilligung ist im Regelfall abzusehen, weil der DSGVO folgend die Nennung des konkreten Verwendungszwecks benötigt wird.

Beispielbox 2: Beispiel aus der Forschung von Jonathan Greenleaf (siehe auch den Band [KA Notizen 84](#)). Jonathan hatte für die Forschung für seine BA Arbeit bereits erste Interviews und Beobachtungen durchgeführt und für diese eine entsprechende Einwilligung von den Forschungspartner:innen eingeholt, als die Idee entstand, BA Arbeiten in einem Aufsatzband zu veröffentlichen. In der Einwilligungserklärung war dies als Verwendungszweck aber nicht angekündigt – hier wurde noch erklärt, dass die Daten „von den Studierenden im Rahmen von Hausarbeiten oder Bachelorarbeiten verwendet werden [können]. Die Forschungsdaten sind nicht öffentlich zugänglich und werden über den Seminkontext hinaus nicht veröffentlicht.“ Um den erweiterten Verwendungszweck der Daten abzusichern, setzte sich Jonathan erneut mit den Forschungspartner:innen in Verbindung und klärte eine Erweiterung der ursprünglichen Einverständniserklärung für die Veröffentlichung ab, die entsprechend dokumentiert wurde.

Form der Einwilligung

Eine Einwilligung kann mündlich, schriftlich oder auch elektronisch (z.B. in einem Webformular) abgegeben werden. Unabhängig vom Grundsatz der Formfreiheit existiert jedoch eine Nachweispflicht. Deshalb wird im Allgemeinen die Schriftform empfohlen. Die Schriftlichkeit stellt außerdem sicher, dass auch zu einem späteren Zeitpunkt noch nachvollziehbar ist, worin eingewilligt wurde. Falls das Einholen einer Einwilligung in Schriftform in der Praxis nicht möglich bzw. nicht angemessen ist – weil beispielsweise bereits die Unterzeichnung eines Formulars ein Risiko für die Forschungspartner:innen darstellen und/oder den Feldzugang verunmöglichen kann –, kann auch eine mündliche Zustimmung eingeholt werden, die z.B. mit Audio/Video aufgezeichnet oder durch Dritte bezeugt werden kann (vgl. Brenner & Löhe 2019). Ist auch das nicht möglich, muss die mündliche Einwilligung zumindest ausreichend dokumentiert werden, indem z.B. Forschende in Feldnotizen oder Postskripten festhalten, wie Information und Einwilligung erfolgt sind. Da noch unklar ist, ob solche Formen der Einwilligung den Anforderungen einer rechtswirksamen Dokumentation genügen, sollte möglichst nur in Ausnahmefällen darauf zurückgegriffen werden. Welche Form der Dokumentation im jeweiligen Kontext angemessen ist, muss gleichwohl von Fall zu Fall entschieden und ggf. auch mit den Forschungsteilnehmer:innen ausgehandelt werden. Gerade in ethnografischer Forschung kann es vorkommen, dass in ein und derselben Forschung Einwilligungen in unterschiedlicher Form dokumentiert werden müssen. Studierende sollten daher das konkrete Vorgehen unbedingt mit Betreuenden bzw. Dozierenden absprechen.

Infobox 4: Inhalte der Informierten Einwilligung. Die Informierte Einwilligung sollte mindestens über Folgendes in klarer Weise informieren (vgl. RatSWD 2023: 17):

- Name und Kontaktdaten der projektverantwortlichen Person(en), ggf. der vertretenden Stelle bzw. des benannten Datenschutzbeauftragten.
- Name und Kontaktdaten der Ansprechperson für Fragen während der Durchführung des Forschungsvorhabens.
- Beschreibung des Forschungsprojektes (Projekttitle, Ziele und konkretes Vorhaben).
- Angaben darüber, welche personenbezogenen Informationen (z.B. Name, Familienzugehörigkeit, Alter) erhoben und verwendet werden. Werden besonders schützenswerte Kategorien personenbezogener Daten (siehe Definitionsbox 1) verarbeitet, so müssen die Forschungsteilnehmer:innen darüber ausdrücklich informiert werden, auch muss der Einwilligungsbogen selbst auf diese besonders schützenswerten Datenarten hinweisen.
- Informationen über die Zweck(e) der Datenverarbeitung: Falls eine Übermittlung oder Weitergabe der Daten an ein Forschungsdatenzentrum zur Archivierung und wissenschaftlichen Nachnutzung geplant ist, muss ausdrücklich darüber informiert werden.
- Hinweise auf die wichtigsten Rechte der Forschungsteilnehmer:innen, insbesondere zur Freiwilligkeit der Teilnahme und zur Möglichkeit des Widerrufs mit Wirkung für die Zukunft sowie der Folgenlosigkeit bei Verweigerung oder Widerruf.
- Ort, Datum, Unterschrift(en).

Eine Informierte Einwilligung als Gesamtdokument besteht idealerweise aus mehreren Teilen (Meyermann & Porzelt 2019: 13; Kretzer et al. 2020: 4), nämlich einem Informationsteil, in dem das Forschungsvorhaben erläutert wird, einem datenschutzrechtlichen Informationsteil, der über die Verarbeitung und Nutzung von personenbezogenen Daten für Forschungszwecke und die Rechte von Betroffenen informiert und schließlich einem Einwilligungsbogen. Die erläuternden Teile der Informierten Einwilligung sollten so spezifisch wie nötig und so allgemein wie möglich formuliert werden.

Informierte Einwilligung in der Praxis

Auch hier gilt: Wie, wann und in welcher Form eine Informierte Einwilligung eingeholt werden kann, hängt wesentlich vom jeweiligen Feld und den konkreten Forschungsbeziehungen ab. In der Literatur finden sich Beispiele, in denen Interaktionsprozesse im Feld durch das Einholen einer mit Unterschrift dokumentierten Einwilligung gestört und Vertrauensbeziehungen zu Forschungsteilnehmer:innen beeinträchtigt worden wären, etwa wenn Forschungsthema und -gegenstand im lokalen Kontext mit einem Stigma behaftet sind (z.B. Dilger 2015). Insbesondere wenn sensible oder auch tabuisierte Themen wie die eigene Krankheit, Schulden oder Gewalt Thema der Forschung sind, ist jedoch eine gute Vertrauensbasis unerlässlich. Gerade die Form der Einwilligung – im Idealfall schriftlich und unterzeichnet – kann bei bestimmten Personengruppen die z.B. bereits Repressionen ausgesetzt sind, zusätzliches Misstrauen wecken, womöglich den Feldzugang erschweren oder gar verhindern. In anderen Kontexten, in denen z.B. formelle Praktiken wie das Unterschreiben von Dokumenten gängig sind oder wenn unterzeichnete Dokumente als vertragliche Garantie dafür aufgefasst werden, dass Vereinbarungen eingehalten werden (z.B. Inhorn 2004), kann das Einholen von schriftlicher Informierter Einwilligung wiederum einen positiven Effekt auf die Forschungsbeziehung zwischen Forscher:in und Forschungsteilnehmer:in haben und eine Vertrauensbasis schaffen.

Infobox 5: Beispiele für Vorlagen und Hilfen für das Einholen der Informierten Einwilligung.

- Das Forschungsdatenzentrum Qualiservice bietet Muster für Einwilligungserklärungen für Forschung und Archivierung/Nachnutzung (deutsch und englisch). Die Muster stehen kostenfrei zum [Download](#) bereit und können an das je spezifische Forschungsvorhaben angepasst werden (FDZ Qualiservice, o.J.).
- Der Verbund Forschungsdaten Bildung hält [Formulierungsbeispiele zur Erstellung von Einwilligungserklärungen](#) u.a. [in leichter Sprache](#) bereit (VerbundFDB, 2018a und 2018b).
- Ein Überblick zu Bedeutung und Verwendung der Informierten Einwilligung in der ethnologischen (Feld-)Forschung findet sich in Huber und Imeri (2021).
- Weitere Überlegungen zu Informierter Einwilligung in digitaler Ethnografie finden sich in Franken (2022: 31–33).

III: Für Datensicherheit sorgen – Technik und Tools

Datensicherheit ist nicht nur ein wesentlicher Teil von Datenschutz, sondern betrifft auch die technischen Voraussetzungen für einen ethisch angemessenen Umgang mit Forschungsdaten. Darüber hinaus gibt es pragmatische Gründe, Fragen der Datensicherheit mit Aufmerksamkeit zu begegnen, um beispielsweise das unbeabsichtigte Löschen von Daten zu vermeiden. Es ist sinnvoll, bereits vor der Datenerhebung bzw. in der Anfangsphase von Haus- und Projektarbeiten zu überlegen, welche organisatorischen wie technischen Maßnahmen zur Sicherung der – insbesondere personenbezogenen – Forschungsdaten angemessen sind. Die Bestimmungen des Datenschutzes und der Datensicherheit können auf den ersten Blick auch erfahrene Forschende entmutigen oder überfordern. Gleichwohl gibt es einige einfache und niedrighschwellige Strategien, den Anforderungen zu begegnen.

Sicher kommunizieren

Bereits bei der Kontaktabbahnung und -aufnahme stellen sich nicht nur praktische und forschungsethische, sondern auch datenschutzrechtliche Fragen. Zur Kommunikation mit Feldakteur:innen, aber z.B. auch mit Projektpartner:innen empfiehlt es sich daher, ausschließlich die E-Mail-Adresse der Universität bzw. der Forschungseinrichtung zu nutzen. Die Verwendung von Messenger-Diensten wie Whatsapp, Telegram usw. sollte möglichst vermieden werden, da hier je nach Nutzungsbedingungen Anbietern der Zugriff auf die Kontaktdaten Dritter ermöglicht wird. Sollten solche Dienste gängige Kommunikationsmedien der Akteur:innen im Feld und deren Nutzung damit nicht vermeidbar sein, ist es wichtig, sich diesen Umstand immer wieder bewusst zu machen und ggf. zusätzliche technische und organisatorische Maßnahmen zu ergreifen, wie z.B. Datenverschlüsselung, die Verwendung sicherer Passwörter oder die Beschränkung des Datenzugriffs.

Grundsätzlich gilt, dass Kontaktdaten von (potentiellen) Gesprächspartner:innen (z.B. Namen, E-Mailadressen oder Telefonnummern) besonders vertraulich behandelt werden müssen. Sie sollten getrennt von den Forschungsdaten aufbewahrt und in der Regel nach Projektende gelöscht werden. Um vor allem sensible Daten und Informationen während des Forschungsprozesses vor unbefugtem Zugriff zu schützen, sollten Dateien und Ordner – unabhängig vom Speicherort sowie beim Versand per E-Mail – verschlüsselt werden.

Infobox 6: Dateien verschlüsseln. Ein sicherer Passwort-Schlüssel sollte mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie Sonderzeichen umfassen, nicht im Wörterbuch stehen und keine Namen, Geburtsdaten oder Autokennzeichen enthalten. Zur Speicherung und Verwaltung von verschiedenen, komplexen Passwörtern empfiehlt sich die Nutzung eines Passwort-Managers.

Nützliche Informationen zu Verschlüsselungstechniken und Tools finden sich im [CES-SDA Data Management Expert Guide](#) (CESSDA Training Team 2020).

Aufzeichnen

Wichtig ist es zunächst, zu überlegen, welche technischen Systeme und Geräte verwendet werden sollen, um Gespräche und anderes aufzuzeichnen. Die Auswahl sollte nicht nur von

den technischen Möglichkeiten (z.B. Tonqualität) und Präferenzen der Forschenden und/oder Forschungspartner:innen abhängig gemacht werden, sondern auch datenschutzrechtliche Überlegungen einschließen.

Auch in der ethnografischen Forschung werden für die Aufzeichnung von Gesprächen, Beobachtungen und Szenen eine Vielzahl an digitalen Tools und mobilen Endgeräten (z.B. Smartphone oder Tablet) verwendet. Die Nutzung privater Endgeräte birgt zahlreiche datenschutzrechtliche Risiken und ist nur eingeschränkt zu empfehlen: So sind privat im Alltag genutzte Smartphones häufig vielfach vernetzt. Damit kann die Gefahr bestehen, dass Ton- und Videomitschnitte (versehentlich oder automatisch) z.B. in Cloud-Dienste hochgeladen oder anderweitig für Dritte zugänglich gemacht werden. Auch Kommunikationstools wie z.B. Zoom standen in der Vergangenheit wegen mangelnder Datenschutzvorkehrungen in der Kritik. Besondere Vorsicht ist daher gerade bei Online-Gesprächen über sensible Themen oder mit vulnerablen Personen geboten. Viele Universitäten geben für die Auswahl und Nutzung von Tools Empfehlungen und Einschätzungen, ob eine Anwendung für den Studienalltag und/oder im Rahmen einer Forschungsarbeit aus datenschutzrechtlicher Sicht zulässig ist.

Daten und Material speichern

Es gibt mittlerweile zahlreiche Möglichkeiten, Daten und Material zu speichern, wie etwa PC und Laptop, mobile Datenträger (z.B. USB-Sticks oder externe Festplatten), Cloud-Dienste (z.B. Dropbox) und institutionelle Netzlaufwerke. Speicherlösungen, die von der jeweiligen Universität zur Verfügung gestellt werden, sollte grundsätzlich der Vorzug gegenüber proprietären Cloud-Diensten und privaten USB-Sticks und Festplatten gegeben werden. Die nachfolgende Abbildung 2 bietet eine kurze Übersicht über die wichtigsten Vor- und Nachteile der einzelnen Speichermedien und -orte.

Aus der Abbildung geht hervor, dass Speichermedium und Speicherorte unterschiedlich gut geeignet sind, gerade, wenn es um den Schutz von sensiblen Informationen geht. So ist es zum Beispiel zwingend notwendig, solche Informationen, die Personen eindeutig identifizieren – z.B. Kontaktdaten, die etwa aufbewahrt werden, um den Feldzugang zu dokumentieren oder wiederholte Kontaktaufnahme zu ermöglichen – so früh wie möglich vom übrigen Material zu trennen und an einem gesonderten Ort zu speichern. Vertrauliche Daten müssen so gespeichert und aufbewahrt werden, dass sie für Unbefugte nicht zugänglich sind.

Neben der sicheren Speicherung ist es auch wichtig, in regelmäßigen Abständen Sicherungskopien der gespeicherten Dateien anzufertigen (vgl. RatSWD 2023: 22; forschungsdaten.info 2023c). So können im Falle eines Datenverlusts, z.B. durch unbeabsichtigtes Über-

Infobox 7: Backup-Strategie. Eine gängige Backup-Strategie ist die sog. *3-2-1-Backup-Regel*: Mindestens 3 Kopien einer Datei auf 2 verschiedenen Speichermedien (z.B. eine Festplatte und eine Cloud) und 1 Backup-Kopie an einem externen Standort („außer Haus“, um Datenverlust durch Brand, Wasserschaden, Einbruch etc. zu vermeiden) (vgl. RatSWD 2023: 22).

schreiben bzw. Löschen von Dateien, durch Virus- bzw. Hackerangriffe oder durch Hardwareschäden, Daten aus einer Sicherung wiederhergestellt und somit Arbeitsschritte rekonstruiert werden. Gerade in Forschungsgruppen oder Gruppenarbeiten empfiehlt es sich, eine gemeinsame Backup-Strategie festzulegen und etwaige Verantwortlichkeiten und Rollen zu klären. An vielen Universitäten bieten die Serviceeinrichtungen bereits Backup-Optionen und -Routinen an, die zum Großteil automatisiert ablaufen und Hilfestellung für die praktische Umsetzung von Maßnahmen zum Schutz und zur Sicherheit der Daten geben. Idealerweise werden unterschiedliche Ziele, Speichermedien und Programme für das Backup verwendet (siehe Infobox 7), damit man im Ernstfall auf der sicheren Seite ist.





Wo speichere ich meine Daten?	
	<p>Eigener PC oder Laptop</p> <ul style="list-style-type: none"> + Maximale Kontrolle + Speicherplatz erweiterbar - Verantwortung für Sicherheit und Backup liegt bei den Forschenden - Kein kollaboratives Arbeiten an Dokumenten - PC-Komponenten können kaputt und Laptops verloren gehen
	<p>Mobile Speichermedien (USB-Stick, externe Festplatte, etc.)</p> <ul style="list-style-type: none"> + Einfach transportierbar + Geringe Kosten + Kein Internetzugang für die Datenübertragung notwendig (z.B. im Feld) + Können einfach eingeschlossen (z.B. Tresor) und/oder verschlüsselt werden - Können leicht kaputt oder verloren gehen - Speicherkapazität ist begrenzt
	<p>Externe Cloud-Dienste (Dropbox, Google Drive, etc.)</p> <ul style="list-style-type: none"> + Einfache Nutzung + Nutzbar für mobiles und kollaboratives Arbeiten + Automatische Backups und Versionierung + Ordner und Dateien können mit Zugriffsbeschränkungen versehen werden - Abhängig vom Zugang zum Internet - Wenig Kontrolle über den Speicherort und Backup-Strategien - Oft unklarer Datenschutz; Universitäten raten häufig von der Nutzung ab
	<p>Institutionelle Speicherorte (Cloud oder virtuelle Laufwerke)</p> <ul style="list-style-type: none"> + Speicherung erfolgt auf Grundlage der Datenschutzbestimmungen + Regelmäßiges Backup ist sichergestellt + Professionelle Administration und Wartung + Ordner und Dateien können mit Zugriffsbeschränkungen versehen werden - Abhängig vom Zugang zum Internet (sofern keine Client-Lösungen angeboten werden) - Können meist nur so lange genutzt werden, wie man selbst Teil der Institution ist.

Abbildung 2: Datenspeicherung

Quelle: In Anlehnung an Biernacka et al. 2018: 63–64 und RatSWD 2023: 21.

Infobox 8: Datenorganisation. Weiterführende Hinweise zu Dateibenennung und Organisation von Daten

- [Tipps für das Anlegen von Ordnerstrukturen und für die Benennung von Dateien und Ordnern](#) (RatSWD 2023: 23–24).
- [Dateien strukturieren. Empfehlungen zur Verzeichnisstruktur und Dateibenennung](#) (Humboldt-Universität zu Berlin, 2022).
- [Dateien benennen und organisieren](#) (VerbundFDB 2018c).

Daten organisieren

Unabhängig von Art und Umfang des Materials hilft – neben einer hierarchischen Ordnerstruktur – auch eine sinnvolle und einheitliche Dateibenennung dabei, den Überblick zu behalten und sich jetzt und in Zukunft im Material zurechtzufinden. Zudem bildet sich darin im Forschungsverlauf zunehmend eine innere Logik des Datenmaterials ab. Dateinamen sollten nicht nur deskriptiv sein und Rückschlüsse auf deren Inhalt erlauben, sondern auch systemübergreifend lesbar sein. Grundsätzlich gilt, dass Leer- und Sonderzeichen – außer Unterstrich und Bindestrich – sowie Umlaute vermieden werden sollen, weil sie bei manchen Betriebssystemen Fehler verursachen können. Bei der Zusammenarbeit in Teams empfiehlt es sich, als Grundlage für einen gemeinsamen sorgfältigen Umgang mit dem Material von Beginn an Regeln für eine einheitliche und konsistente Benennung festzulegen.

Eine Dateibezeichnung, die im Rahmen des Studiums entsteht, könnte z.B. so aussehen und sich aus folgenden Bausteinen zusammensetzen:

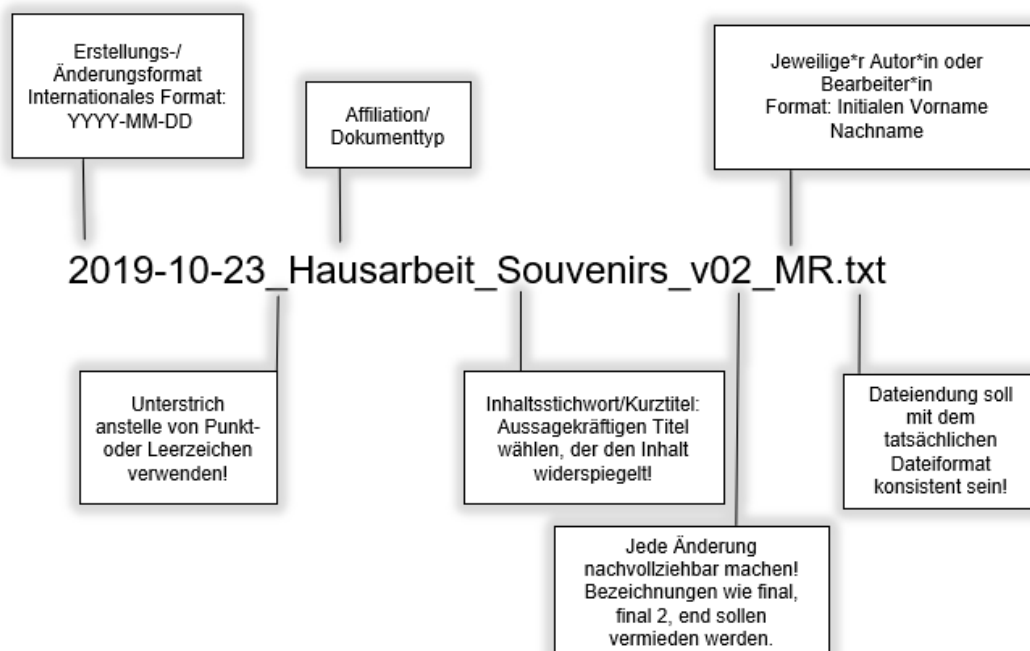


Abbildung 3: Benennungskonvention für Dateinamen am Beispiel einer Hausarbeit.

Quelle: Eigene Abbildung.

Daten teilen

Innerhalb eines Forschungsteams oder auch im Rahmen von Lehrforschungsprojekten kann es notwendig sein, sich darüber zu verständigen, welche Materialien in welcher Form mit anderen geteilt werden sollen oder müssen. Während pseudonymisierte bzw. anonymisierte Transkripte und Postskripte von Interviews im Projektzusammenhang mit Blick auf den Datenschutz problemlos untereinander geteilt werden können, kann es vorkommen, dass z.B. Feldnotizen oder Audio-Aufnahmen nicht mit anderen im Projekt geteilt werden können oder sollen, weil sie nur schwer und mit großem Aufwand zu anonymisieren sind.

Auch wenn Daten ausschließlich innerhalb von Forschungsgruppen oder im Seminar geteilt werden, gilt es, auf die Sicherheit der Daten zu achten und diese vor Fremdzugriff zu schützen. Hierfür empfiehlt sich die Nutzung universitätseigener Datenspeicher und Cloud-Anwendungen. Services externer Anbieter wie Dropbox, Google Drive oder vergleichbare kommerzielle Cloud-Lösungen sollten hingegen nicht genutzt werden, da die Sicherheit der Daten nicht gewährleistet wird. Daten bzw. Datei-Dokumente sollten mittels eines Passworts verschlüsselt werden.

Daten löschen

Neben der Sicherung von Daten mit Personenbezug kann auch das Löschen eine Maßnahme der Datensicherheit und des Datenschutzes darstellen. In der Regel verlangt das Datenschutzrecht die Löschung personenbezogener Daten, sobald der Verwendungszweck (z.B. eine Forschung im Rahmen der Masterarbeit oder eine Publikation) erfüllt ist bzw. wenn die Speicherung der Daten nicht mehr notwendig ist.

Beispielbox 3: Beispiel aus der Forschungspraxis. Ein Institut stellt Studierenden im Rahmen eines Lehrforschungsprojektes zum Thema „Spiele(n) im Alter“ verschiedene technische Geräte und Zubehör zur kostenlosen Nutzung zur Verfügung. Mika – Student:in im Masterstudiengang Europäische Ethnologie – plant, im Rahmen des Forschungsprojektes Gespräche mit älteren Personen aus dem persönlichen Bekanntenkreis zu führen. Zur Aufzeichnung der Gespräche leiht sich Mika ein Aufnahmegerät vom Institut. Beim Überspielen der Interviewaufnahmen auf einen sicheren Speicherort stellt Mika fest, dass noch weitere Dateien und Aufnahmen auf dem Gerät vorhanden sind. Im Gespräch mit Kommiliton:innen stellt sich heraus, dass die Aufnahmen von Andrea sind, der/die die Dateien zwar sicher abgelegt, jedoch versehentlich vergessen hatte, sie vom Aufnahmegerät zu löschen.

Sofern eine Einwilligung zur Verarbeitung von personenbezogenen Daten vorliegt oder Maßnahmen zur Pseudonymisierung bzw. Anonymisierung (siehe unten) durchgeführt worden sind, kann auf das Löschen der Daten während und ggf. auch nach Projektende verzichtet werden. Damit Daten, die zu einem späteren Zeitpunkt womöglich noch benötigt werden, nicht ungewollt verloren gehen, sollte das endgültige Löschen wohl überlegt sein und ggf. auch mit den Betreuenden von Qualifikationsarbeiten besprochen und etwaige Aufbewahrungspflichten geprüft werden.

Gleichzeitig gibt es im Forschungsalltag immer wieder Momente, in denen das sichere Löschen von Material notwendig und gewünscht ist, etwa wenn Videos, Fotos oder Dokumente von der Festplatte oder vom Speicher eines Smartphones entfernt werden sollen. Z.B. müssen Daten nach der Übertragung auf einen sicheren Speicherort von den Aufnahmegegeräten bzw. Endgeräten in jedem Fall vollständig gelöscht werden. Auch Datenkopien bzw. Backups, die im Rahmen der Datensicherung entstehen, müssen bei der Löschung berücksichtigt werden. Um Daten sicher zu entfernen, reicht das „normale“ Löschen nicht aus – bei sensiblen Daten können weitere Maßnahmen erforderlich sein. So sollten etwa Daten auf Festplatten nicht nur gelöscht, sondern mit geeigneter Software überschrieben und somit vollständig und nicht wiederherstellbar beseitigt werden.

IV: Informationen verfremden - Pseudonymisierung und Anonymisierung

Hat man das Notwendige für die (technische) Sicherheit von Daten getan, können weitere Schritte erforderlich sein, um im Material selbst personenbezogene Informationen zu schützen, die Rechte beteiligter Personen zu wahren und damit gleichzeitig Vertraulichkeitszusagen einzuhalten sowie allgemeiner den ethischen Prinzipien der ethnografischen Forschung gerecht zu werden. In diesem Sinne sind – ähnlich wie die Informierte Einwilligung – Verfahren der Pseudonymisierung bzw. Anonymisierung kein Selbstzweck, sondern aus Sicht des Datenschutzes Verfahren der Verfremdung, die die Speicherung und Verarbeitung personenbezogener Informationen ermöglichen. Im Fachverständnis beschreibt Pseudonymisierung zunächst den Schritt, mit dem in Vorträgen oder Publikationen die Identifikation der Forschungspartner:innen durch Vergabe eines Pseudonyms (der Klarname wird meist durch einen anderen Namen ersetzt) verhindert oder zumindest erschwert werden soll. Wenn also in einem ethnografischen Text bei der Nennung einer interviewten Person beispielsweise in der Fußnote erklärt wird, dass die Person pseudonymisiert wurde, verweist das auf diese fachspezifische Praxis. Der Begriff der Anonymisierung wird im Fachgebrauch meist synonym verwendet.

Im Datenschutzrecht hingegen definieren die Begriffe Anonymisierung und Pseudonymisierung unterschiedliche Grade der Entkoppelung von personenbezogenen Informationen und der betreffenden Person selbst (siehe Definitionsbox 2).

Im Prozess der Anonymisierung werden einzelne personenbezogene Informationen so verändert, dass die betreffenden Personen – Forschungsteilnehmer:innen oder auch etwaige Dritte, über die gesprochen wird – nicht mehr oder nur mit unverhältnismäßigem Aufwand identifiziert werden können. Dabei muss beachtet werden, dass neben dem Namen womöglich andere, auch eher unscheinbare Informationen oder auch Kombinationen etwa aus Alter, Arbeits- und Wohnort Rückschlüsse auf eine Person ermöglichen. Nach der Anonymisierung gelten Daten nicht mehr als personenbezogen und unterliegen deshalb auch nicht länger den Regulierungen des Datenschutzrechts, könnten also aus rechtlicher Sicht z.B. ohne weitere Vorkehrungen veröffentlicht werden.

Unterschieden werden darüber hinaus verschiedene Anonymisierungsgrade: Bei der sog. absoluten Anonymisierung werden neben den direkten Identifikatoren – z.B. Name, Anschrift, Geburtsdatum – auch alle indirekten Identifikatoren – z.B. Angaben zum Arbeitgeber oder zum Krankheitsverlauf – aus dem Material beseitigt oder verändert. Das ist für viele Szenarien ethnografischer Forschung schwierig, weil damit auch ein großer Teil der für die Analyse relevanten Informationen über Personen und Kontexte getilgt würde. Bei der sog.

Definitionsbox 2: Pseudonymisierung und Anonymisierung. Nach der DSGVO bedeutet Pseudonymisierung „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)

Im Gegensatz dazu findet sich in der DSGVO keine eindeutige Definition der Anonymisierung. Sie stellt lediglich klar (Erwägungsgrund 26 DSGVO), dass die Grundsätze des Datenschutzes nicht auf anonyme Informationen angewendet werden. Die DSGVO nimmt dennoch Bezug auf das Konzept der Anonymisierung (vgl. RatSWD 2020: 18) und legt nahe, dass Daten als anonym gelten, wenn sie faktisch anonymisiert sind, d.h. „wenn ein Personenbezug nur mit unverhältnismäßig hohem Aufwand wiederhergestellt werden kann“ (ebd., vgl. hierzu auch Mozygemba & Hollstein 2023). Datenschutzrechtlich liegt der Unterschied also vor allem darin, dass bei Pseudonymisierung über eine Schlüsseldatei Daten einer Person wieder zugeordnet werden können, während diese Möglichkeit bei der Anonymisierung nicht mehr besteht.

faktischen Anonymisierung werden hingegen nur die direkten Identifikatoren ersetzt, zusätzlich muss der oben genannte „unverhältnismäßige Aufwand“ für eine mögliche Re-Identifikation abgewogen werden. Die Herstellung faktischer Anonymität ist der Versuch, die Wahrscheinlichkeit einer De-Anonymisierung nahezu auszuschließen und gleichzeitig den Informationsgehalt der Daten weitgehend zu erhalten.

Auch bei der Pseudonymisierung werden Informationen so verändert, dass eine Person nicht unmittelbar identifiziert werden kann. Im Material ersetzt oder entfernt werden direkt identifizierende Merkmale wie Namen und Adressen. Gleichzeitig werden diese Informationen aber vom Material getrennt – z.B. in einer gesonderten Schlüsseldatei an einem anderen und gesicherten Speicherort – aufbewahrt und damit eine Re-Identifikation ermöglicht. Ein solches Verfahren ist erforderlich, wenn z.B. in einer Langzeitstudie dieselben Personen zu einem späteren Zeitpunkt nochmals befragt werden sollen. Beide Verfahren – Anonymisierung und Pseudonymisierung – sind geeignet, den Grundsätzen des Datenschutzes gerecht zu werden (Baumann et al. 2021: 176–179).

Weil ethnografische Forschung immer auch kontextspezifisch ist, meist auf kleinen Fallzahlen basiert und Material in der Regel zunächst von derselben Person analysiert wird, die es auch erzeugt hat, sind Informationen über Gesprächspartner:innen aus der Sicht der Feldforscher:in kaum anonymisierbar. Die Forscher:in wird also Informationen in aller Regel an die Person zurückbinden können, auf die sie sich beziehen. Mit Blick auf mögliche Leser:innen von Publikationen oder wenn Material aus Forschungsdatenarchiven von Forscher:innen nachgenutzt wird, die nicht selbst an der Forschung beteiligt waren, stellt sich das in der Regel anders dar. Personenbezug kann sich also in Relation zur Person, die Forschungsmaterial benutzt oder rezipiert, verändern (Baumann et al. 2021: 175). Die Antwort auf die Frage, wann und in welchem Umfang ethnografische Forschungsdaten anonymisiert oder pseudonymisiert werden sollten, hängt also auch davon ab, an welchem Punkt im Datenlebenszyklus sie gestellt wird. Insgesamt ist die Grenze zwischen personenbezogenen Daten und pseudonymisierten oder anonymisierten Daten fließend.

Wege der Pseudonymisierung und Anonymisierung

Strategien der Pseudonymisierung und Anonymisierung müssen angesichts der Heterogenität der Forschungsfelder feldspezifisch angepasst werden und sind in der Regel Ergebnis von Aushandlungen mit Gesprächspartner:innen über die Sensibilität von Informationen und damit verbundene mögliche Risiken (Imeri & Huber 2023: 92–98). Zunächst besteht immer auch die Möglichkeit, mit Gesprächspartner:innen zu vereinbaren, dass ihr Klarname und damit der Personenbezug explizit offengelegt werden kann oder gar soll. Denn nicht immer wollen Akteur:innen im Forschungsfeld anonym bleiben oder verfolgen im Rahmen einer Forschung eigene Absichten. Auf Anonymisierung zu verzichten, kann z.B. sinnvoll und in manchen Fällen auch unvermeidbar bei Personen sein, die im öffentlichen Leben stehen oder die als Funktionsträger:in einer Institution interviewt werden, und deshalb leicht erkennbar sein können. In jedem Fall müssen solche Vereinbarungen in der Einwilligungserklärung dokumentiert werden.

In allen anderen Fällen sollten direkte Identifikatoren möglichst frühzeitig aus dem Material entfernt bzw. durch Äquivalente ersetzt werden. Bei der Arbeit z.B. mit Interviews kann es hilfreich sein, bereits bei der Transkription Eigennamen durch Kürzel, Pseudonyme oder IDs zu ersetzen, diese zu kennzeichnen oder sensible Textpassagen zu markieren. Zu beachten ist zudem, dass Informationen über Dritte enthalten sein können, die dann analog maskiert werden müssten. Die Pseudonymisierung bzw. Anonymisierung ethnografischer Daten – auch wenn sie z.B. in Publikationen verwendet werden – kann darüber hinaus weiterführende Strategien erfordern, wie etwa die Vergrößerung, Auslassung oder Veränderung von potenziell identifizierenden Details, wie Orten, Institutionen oder Berufen – eben weil die Kombination mehrerer Merkmale Rückschlüsse auf Personen zulassen kann. Verfremdungsstrategien sollten aber gerade in ethnografischen Texten so eingesetzt werden, dass die Lesbarkeit erhalten bleibt, d.h. dass in der Regel vergleichbare Namen und Bezeichnungen gefunden werden, die den Lesefluss und das Verständnis nicht irritieren.

Infobox 9: Hilfen für die Anonymisierung und Pseudonymisierung

- Der Verbund Forschungsdaten Bildung stellt nützliche Informationen für die praktische Umsetzung und konkrete Beispiele für die Ersetzung einzelner Merkmale von Personen zur Verfügung (Meyermann & Porzelt 2014).
- Das Anonymisierungstool QualiAnon (Nicolai et al. 2021) unterstützt Forschende bei der Anonymisierung/Pseudonymisierung von Textdaten. QualiAnon wurde im Forschungsdatenzentrum Qualiservice als Open Source Software entwickelt und kann kostenfrei von Forschenden genutzt werden. Weiterführende Informationen finden sich auf der [Webseite](#) (FDZ Qualiservice o.J.).

Sehr viel schwieriger ist die Pseudonymisierung bzw. Anonymisierung von Multimediaaldaten (Bild, Audio, Video). So ist die Stimme – ähnlich wie der Fingerabdruck einer Person – einzigartig und kann ggf. zur zweifelsfreien Identifizierung von Personen führen. Verlässliche Verfahren, die eine Stimme derart verfremden, dass diese nicht oder nur unter erheblichem Aufwand zu einer Re-Identifizierung der Person führen, sind aktuell jedoch noch nicht verfügbar. Verwischen oder Verpixeln sind gängige Techniken der digitalen Nachbearbeitung, wenn z.B. Fotos von identifizierbaren Personen in Publikationen verwendet werden sollen. Gleichzeitig wird die Interpretierbarkeit durch solche Maßnahmen in besonderem

Maße beeinträchtigt. Weil Bild-, Audio- und Videodaten aus den genannten Gründen – wenn überhaupt – nur begrenzt anonymisierbar sind, sollte hier ein besonderes Augenmerk auf der sicheren Aufbewahrung liegen.

Material zu anonymisieren oder zu pseudonymisieren ist kein rein ‚mechanischer‘ Vorgang, sondern auch ein kreativer Prozess, der von den Routinen, Erfahrungswerten und Vorlieben der Forscher:in abhängt und sich in unterschiedlicher Weise auf die Arbeit mit dem Material auswirken kann. Die Verwendung von Pseudonymen für Personen kann als distanzierender Schritt von diesen Personen empfunden werden, als Verlust (Van den Hoonaard 2004: 271) genauso wie als Erschaffung von „Figuren eigenständiger Realität“ (Bodner 2018: 62). Überdies können sich die gewählten Pseudonyme oder Ersetzungen auch auf die Wahrnehmung von Leser:innen auswirken, weil sie neue Bedeutungen und Assoziationen generieren. Insbesondere bei größeren Materialkorpora können Schritte der Anonymisierung komplex und aufwändig sein. Grundsätzlich gilt: Um die Dichte ethnografischer Beobachtungen und Beschreibungen und die für das Verständnis so wichtigen Kontexte zu erhalten, sollte so wenig wie möglich, aber immer so umfassend wie für den Schutz der Interessen von Gesprächspartner:innen notwendig, anonymisiert werden.

Schon in prädigitalen Zeiten war Anonymität ein Versprechen, das Ethnograf:innen nicht immer vollständig einlösen konnten, etwa wenn Dritte aktiv versuchten, Orte und Protagonist:innen einer Forschung zu re-identifizieren (vgl. Scheper-Hughes 2000). In Anbetracht fortschreitender Digitalisierung wird zusehends unklarer, wie Anonymität hergestellt werden kann (Shklovski & Vertesi 2013; Bachmann et al. 2017) und ob sich Rückschlüsse auf beteiligte Institutionen und Personen oder auch Orte künftig noch vermeiden lassen (Murphy 2021: 42; Unger 2014: 25). Auch wenn diese Szenarien und damit verbundene Risiken real sind, verweisen sie zunächst einmal auf die Notwendigkeit, mit Daten verantwortungsvoll und sorgsam umzugehen und neben Schritten der Pseudonymisierung und Anonymisierung weitere Schutz- und Sicherungsmaßnahmen in Betracht zu ziehen. Sollen ethnografische Forschungsdaten etwa im Rahmen größerer Forschungsvorhaben archiviert werden, sind meist gute Anonymisierungskonzepte notwendig. Zudem sollten geeignete Datenzentren und Repositorien gewählt werden, die Verfahren der Anonymisierung unterstützen und zusätzlich weitere Schutzmaßnahmen wie etwa abgestufte Zugangsbeschränkungen und die Festlegung von Sperrfristen anbieten.

Beispielbox 4: Forschungsdaten bei Qualiservice anonymisieren. Das Anonymisierungskonzept des Forschungsdatenzentrums Qualiservice ersetzt sensible Informationen durch sozialwissenschaftlich relevante Informationen, damit der Informationsgehalt sowie die Nutzbarkeit der qualitativen Daten möglichst erhalten bleiben. So werden z.B. konkrete Ortsnamen nicht zu Stadt A oder B, sondern zu Wohnort A - eine Großstadt im Norden Deutschlands. Das Abstraktionslevel der Anonymisierung bzw. Pseudonymisierung hängt dabei vom jeweiligen Forschungsvorhaben und der Sensitivität der Daten ab. Praktische Hilfestellung zur Anonymisierung und Pseudonymisierung qualitativer Forschungsdaten bieten die Handreichung von Kati Mozygemba und Betina Hollstein (2023) sowie das Anonymisierungskonzept von Susanne Kretzer (2013).

Forschungsdaten dauerhaft archivieren

FDM zielt nicht nur auf die Planung und den sorgsamsten Umgang mit Forschungsdaten während eines Projekts, sondern auch auf den langfristigen Erhalt von Forschungsdaten. Sie sollen, wo immer möglich, mit anderen Wissenschaftler:innen geteilt und für weitere Forschung zur Verfügung gestellt werden. Das bedeutet nicht zwangsläufig, dass sie im Internet frei zugänglich sein sollen. Vielmehr sollen Forschungsdaten gemäß der sog. FAIR-Prinzipien (siehe Definitionsbox 3) so aufbereitet und gespeichert werden, dass sie von anderen – Menschen und Maschinen – gefunden und nachgenutzt werden können.

Definitionsbox 3: FAIR Prinzipien. Nach den FAIR-Prinzipien sollen Forschungsdaten auffindbar (*findable*), zugänglich (*accessible*), interoperabel (*interoperable*) und wiederverwendbar (*reusable*) sein (Wilkinson et al. 2016).

Im Unterschied zu Konzepten von Open Data, die auf freie Nutzung ohne jegliche Einschränkung zielen, kann die Umsetzung der FAIR-Prinzipien auch bedeuten, dass Daten nur eingeschränkt zugänglich sind.

Eine solche Archivierung von Forschungsdaten aus ethnografischen Forschungen und vor allem Formen der weiteren Nutzung sind in Deutschland nach wie vor keine gängige Praxis. Gleichwohl haben wissenschaftspolitische Akteur:innen und Förderinstitutionen in den letzten Jahren Anforderungen an in diesem Sinne nachhaltiges Forschungsdatenmanagement formuliert. Die Deutsche Forschungsgemeinschaft (DFG) z.B. erwartet, dass bereits bei Antragstellung für ein Projekt der Umgang mit Forschungsdaten beschrieben wird und Forschungsdaten für zehn Jahre in der Einrichtung, in der sie entstanden sind, aufbewahrt werden (DFG 2022: 22). Archivierung meint dabei zunächst die langfristige Speicherung oder auch Langzeitarchivierung von Daten und Material und geht damit über das reine Backup (siehe Infobox 7) hinaus – auch wenn der zeitliche Umfang von ‚Langzeitarchivierung‘ nicht einheitlich definiert ist. Daten müssen dabei lesbar gehalten werden, z.B. auch über etwaige Dateiformatänderungen hinweg. Auch wenn studentische Forschungen Teil von Prüfungsleistungen sind, müssen die dafür verwendeten Daten für einen bestimmten Zeitraum aufbewahrt werden, in der Regel für fünf Jahre. Die genauen Aufbewahrungsfristen sollten aber unbedingt mit der Lehrperson bzw. dem Prüfungsausschuss geklärt werden. Das gilt auch für die Frage, wie die Daten in dieser Zeit angemessen aufbewahrt werden und wer ggf. für die spätere Löschung zuständig ist.

Um Forschende in diesem Prozess zu unterstützen, bieten Forschungseinrichtungen im Regelfall Verfahren, Werkzeuge und Infrastrukturen zur langfristigen Aufbewahrung von Daten an und/oder entwickeln entsprechende Beratungsangebote. Die Speicherung kann dabei auf unterschiedlichen Ebenen bzw. mit unterschiedlichen Zielsetzungen erfolgen: Zur reinen Aufbewahrung werden die Daten etwa auf Magnetbändern gespeichert und sicher in mehreren Kopien an räumlich getrennten Standorten erhalten. Sie sind dort nicht im Sinne der FAIR-Prinzipien verfügbar und in der Regel nur für die Forscher:in und ggf. technisches Personal zugänglich (*dark archiving*). Damit kann z.B. der von der DFG geforderten Aufbewahrungsfrist von mindestens zehn Jahren Genüge getan werden. Darüber hinaus betreiben viele Universitäten mittlerweile öffentlich zugängliche Repositorien für die Publikation von Forschungsdaten (z.B. aus abgeschlossenen Projekten oder Abschlussarbeiten). Sie stehen in

der Regel allen Universitätsangehörigen zur Verfügung – auch Studierenden. Forschungsdaten sind hier in der Regel frei verfügbar, ggf. auch mit niedrighwelligen Zugangshürden versehen. Mit Blick auf die Spezifik ethnografischer Materials ist eine Veröffentlichung ganzer Datenkonvolute – über die datenschutzkonforme wie ethisch angemessene Verwendung von Auszügen in Publikationen hinaus – in solchen Repositorien in der Regel nicht möglich.

Für viele Fachgebiete bzw. Datentypen und Materialarten wurden in den letzten Jahren zudem spezialisierte Fachrepositorien bzw. Forschungsdatenzentren aufgebaut. Das sind Institutionen mit disziplin- und datenspezifischer Expertise, die häufig zusätzliche Services wie z.B. inhaltliche Qualitätsprüfung, Prüfung der Anonymisierung oder die Kuration von Metadaten anbieten. In vielen Fällen steht hier die Aufbereitung von Forschungsdaten für weitere Nutzungen im Vordergrund. Für ethnografische Forschungsdaten werden seit 2019 bei Qualiservice – dem Forschungsdatenzentrum für qualitative sozialwissenschaftliche Daten – und in Kooperation mit dem Fachinformationsdienst Sozial- und Kulturanthropologie (FID SKA) angemessene Archivierungslösungen und Services erarbeitet, um Material aus ethnografischer Forschung unter kontrollierten Bedingungen archivieren und zur Nachnutzung bereitstellen zu können.

Unabhängig davon, in welcher Institution und mit welchem Ziel ethnografische Forschungsdaten langfristig archiviert werden sollen: Vorab sollte eingehend geprüft und im Rahmen von Qualifizierungsarbeiten gemeinsam mit der betreuenden Person abgewogen werden, ob und wenn ja, unter welchen Bedingungen eine Archivierung sinnvoll und möglich ist. Auch FDM-Personal an Universitäten (z.B. Abteilungen oder Stellen für Forschungsdatenmanagement, Data Stewards etc.) und/oder Universitätsbibliotheken können als beratende Instanzen Unterstützung bieten. Das Forschungsdatenzentrum Qualiservice empfiehlt ethnografisch Forschenden, möglichst frühzeitig Kontakt aufzunehmen, auch weil die Archivierung dort mit Kosten verbunden ist. Darüber hinaus sollten Schritte der Dokumentation und Datenvorbereitung bereits von Anfang an mitgedacht und in den Forschungsprozess integriert werden. Bei Qualiservice werden Forschende dabei stets von Fachwissenschaftler:innen begleitet und unterstützt (Rizzolli et al. 2023).

Auch wenn es also mittlerweile spezialisierte Einrichtungen für die Archivierung qualitativer wie ethnografischer Forschungsmaterialien gibt, stehen Archivierung und Bereitstellung, aber auch die Nachnutzung solcher Daten und Materialien bisher noch am Anfang. Dass Ansätze der Sekundäranalyse – also einer erneuten Auswertung von archivierten Forschungsdaten – aber mehr Aufmerksamkeit gewinnen, zeigt z.B. der Beitrag von Franken et al. in diesem Band. Insgesamt sind verschiedene Möglichkeiten und Szenarien der Nachnutzung denkbar: Archivierte Forschungsdaten könnten etwa unter einer neuen Fragestellung oder einer neuen Forschungsperspektive analysiert werden. Bereits bestehende Daten und Kontextmaterialien (z.B. Leitfäden, Transkriptionsregeln) können aber auch in der Lehre – etwa in der Methodenausbildung – verwendet werden und bieten Möglichkeiten zur Sensibilisierung von Studierenden für Forschungsethik, Datenschutz und Forschungsdokumentation. Die Nachnutzung bestehender Forschungsmaterialien kann in diesem Sinne auch einen wichtigen Beitrag zur Methodenentwicklung leisten.

Schlussbemerkungen

Forschungsdatenmanagement umfasst unterschiedliche Ebenen und vielfältige Schritte, die die Generierung, Verarbeitung und weitere Nutzung von Forschungsdaten begleiten. Wir

haben in diesem Beitrag einige aus unserer Sicht zentrale Aspekte des FDM beschrieben sowie einführende Informationen und konkrete Hinweise für die Umsetzung gegeben. Im Zentrum standen dabei Fragen, die während des eigentlichen Forschungsprozesses relevant sind. Weitergehende Schritte, die mit der Archivierung und vor allem der Vorbereitung für eine spätere Nachnutzung notwendig werden, haben wir hingegen nur als Ausblick behandelt. Unsere Schwerpunktsetzungen haben auch damit zu tun, dass die hier adressierte Leserschaft in erster Linie Studierende sind, die im Rahmen ihrer Forschungen zum ersten Mal mit Fragen von Datenschutz, Datensicherheit und Ähnlichem konfrontiert sind und eine ethnografischen Zugängen und ethnografischer Forschungspraxis adäquate praktische Handreichung benötigen. Entsprechend verstehen wir den Beitrag als orientierende Einführung für Studierende, die – so unsere Hoffnung – aber auch für Promovierende und Forschende allgemein hilfreich sein kann.

Es war im Rahmen, den der Band insgesamt vorgegeben hat, nicht möglich, alle Themen und Aspekte im Detail zu besprechen, die wir mit Blick auf die Debatten zum Forschungsdatenmanagement, aber auch mit Blick auf die konkrete Praxis des Umgangs mit Daten für relevant halten. Die zahlreichen Links, Referenzen und Hinweise auf weiterführende Literatur sollen es Leser:innen ermöglichen, das Thema insgesamt, aber auch in einzelnen Aspekten weiter zu vertiefen.

Wir schließen den Beitrag mit einigen zentralen Hinweisen: Gerade ethnografisch Forschende machen derzeit vielfältige Erfahrungen mit Forschungsdatenmanagement und insbesondere rechtlichen und ethischen Fragen, die in den nächsten Jahren zu einer Anreicherung mit weiteren Vorschlägen und praktischen Ergänzungen für unseren Fachzusammenhang führen werden. Das gilt nicht nur, aber insbesondere in genuin digitalen bzw. Online-Forschungsfeldern. Hinzu kommen fortlaufende infrastrukturelle Entwicklungen bei Qualiservice und anderswo, die Forschende zukünftig mit weiteren Services unterstützen können. Und auch das Datenschutzrecht unterliegt einer kontinuierlichen Weiterentwicklung und Konkretisierung, so dass die in diesem Beitrag gegebenen Empfehlungen und Informationen nur über eine bedingte ‚Haltbarkeit‘ verfügen. Gerade mit Blick auf die Online-Forschung sind einige rechtliche Fragen noch nicht annähernd geklärt. Insofern bildet der Beitrag einen Stand zu einem Zeitpunkt ab, und es gilt, Debatten, Erfahrungen und neue Entwicklungen im Blick zu behalten, die das hier Formulierte sinnvoll ergänzen werden.

Bestehen bleiben wird die Notwendigkeit, Anforderungen, die von Fördergebern gestellt werden oder die aufgrund rechtlicher Vorgaben entstehen, mit Blick auf ihre Passfähigkeit für die ethnografische Forschung insgesamt zu hinterfragen, gleichzeitig aber auch einzelne Schritte des Datenmanagements immer wieder für den je spezifischen Einzelfall auf ihre Angemessenheit hin zu überprüfen. Hier gilt – wie für den gesamten ethnografischen Forschungsprozess generell –, dass auch für das FDM forschungsethische Fragen leitend sind, die über gesetzlich geregelte datenschutzrechtliche Prinzipien hinausgehen können. Deshalb ist eine grundlegende Kenntnis gerade der rechtlichen Rahmenbedingungen notwendig, um entsprechende Anpassungen für den spezifischen Forschungsgegenstand zu entwickeln. Gleichzeitig ist es erforderlich, mit Blick auf das konkrete Forschungsfeld, vor allem aber mit Blick auf die Möglichkeiten und Risiken digitaler Datenverarbeitung die ethische Urteilskraft zu stärken – am besten im Austausch mit Kolleg:innen, Betreuer:innen, Peers. Aus dieser einzelfallspezifischen Auseinandersetzung mit den unterschiedlichen Aspekten und Schritten des FDMs erhoffen wir uns künftig nicht zuletzt eine kritische Reflexion unserer disziplinär geprägten Daten-Ideologien. In diesem Sinne ist dieser Beitrag ähnlich wie der

Datenmanagementplan ein lebendes Dokument, das an anderen Stellen weiterentwickelt werden wird.

Anmerkungen

Für kritisches Lesen des Textes in unterschiedlichen Stadien der Ausarbeitung, hilfreiche Anmerkungen und Vorschläge zur Verbesserung danken wir – neben den Herausgeber:innen und den Mitautor:innen des Bandes – in alphabetischer Reihenfolge: Esther Asef, Eva Ommert, Franz Templin und Cosima Wagner.

Literatur

- Bachmann, Götz, Michi Knecht & Andreas Wittel (2017): The Social Productivity of Anonymity. Introduction. In: *Ephemera: Theory & Politics in Organization* 17/2, 241–258. https://irep.ntu.ac.uk/id/eprint/31952/1/PubSub9418_Wittel.pdf. Letzter Zugriff: 22.08.2023.
- Baumann, Paul, Philipp Krahn & Anne Lauber-Rönsberg (2021): *Forschungsdatenmanagement und Recht. Datenschutz-, Urheber- und Vertragsrecht*. Feldkirch/Düns: Wolfgang Neugebauer Verlag.
- Benner, Angela & Julian Löhe (2019): Die informierte Einwilligung auf Tonband: Analyse im Rahmen einer qualitativen Interviewstudie mit älteren Menschen aus forschungsethischer und rechtlicher Perspektive, *ZQF – Zeitschrift für Qualitative Forschung* 2, 341–356. <https://doi.org/10.3224/zqf.v20i2.08>.
- Biernacka, Katarzyna, Dominika Dolzycka, Kerstin Helbig & Petra Buchholz (2018): Train-the-Trainer Konzept zum Thema Forschungsdatenmanagement. <https://doi.org/10.5281/zenodo.1215377>.
- Bodner, Reinhard (2018): *Berg/Leute: Ethnografie eines ausgebliebenen Bergsturzes am Eiblschrofen bei Schwaz in Tirol (1999)*. Münster: Waxmann.
- CESSDA [Consortium of European Social Science Data Archives] (2019): *Adapt your Data Management Plan: A List of Data Management Questions Based on the Expert Tour Guide on Data Management*. https://static-archive.CESSDA.eu/content/download/4302/48656/file/TTT_DO_DMPExpertGuide_v1.3.pdf. Letzter Zugriff: 14.07.2023.
- CESSDA Training Team (2020): *CESSDA Data Management Expert Guide*. Bergen. CESSDA ERIC. <https://doi.org/10.5281/zenodo.3820473>.
- Cliggett, Lisa (2020): Post-script: Thoughts on Data Lifecycle and the Lifecycle of Anthropological Thought on Data. In: Jerome W. Crowder, Mike Fortune, Rachel Besare & Lindsay Poirier (Hgs.), *Anthropological Data in the Digital Age. New Possibilities – New Challenges*. Cham: Palgrave Macmillan, 255–265. https://doi.org/10.1007/978-3-030-24925-0_12.
- DFG [Deutsche Forschungsgemeinschaft] (2022): *Leitlinien zur Sicherung guter wissenschaftlicher Praxis. Kodex. 1.1.* <https://doi.org/10.5281/zenodo.6472827>.
- DFG-Fachkollegium 106 Sozial- und Kulturanthropologie, Außereuropäische Kulturen, Judaistik und Religionswissenschaft (2020): *Handreichung zum Umgang mit Forschungsdaten*. https://www.dfg.de/download/pdf/foerderung/grundlagen_dfg_foerderung/forschungsdaten/handreichung_fachkollegium_106_forschungsdaten.pdf. Letzter Zugriff: 14.07.2023.

- DGEKW [Deutsche Gesellschaft für Empirische Kulturwissenschaft, vormals Deutsche Gesellschaft für Volkskunde dgv] (2018): Positionspapier zur Archivierung, Bereitstellung und Nachnutzung von Forschungsdaten. https://dgek.w.de/wp-content/uploads/2023/03/dgv-Positionspapier_FDM.pdf. Letzter Zugriff: 14.07.2023.
- DGSKA [Deutsche Gesellschaft für Sozial- und Kulturanthropologie] (2019): Positionspapier zum Umgang mit ethnologischen Forschungsdaten. https://www.dgska.de/wp-content/uploads/2019/11/Positionspapier_Bearbeitet-fu%CC%88r-MV_24.09.2019.pdf. Letzter Zugriff: 14.07.2023.
- Dilger, Hansjörg (2015): Ethik und Ethnologie. Ethikkommissionen, ethnographisches Arbeiten und Epistemologie – nicht nur in der Medizinethnologie. Blogbeitrag zu: Medizinethnologie. Körper, Gesundheit und Heilung in einer globalisierten Welt, (16.09.2015). <https://www.medizinethnologie.net/2015/09/>. Letzter Zugriff: 31.03.2023.
- EASA [European Association of Social Anthropologists] (2018): EASA's Statement on Data Governance in Ethnographic Projects, <https://www.easaonline.org/downloads/support/EASA%20statement%20on%20data%20governance.pdf>. Letzter Zugriff: 14.07.2023.
- EVIFA – Fachportal Ethnologie (o.J.): Forschungsdaten. <https://www.evifa.de/de/forschungsdaten>. Letzter Zugriff: 16.07.2023.
- FDZ Qualiservice [Forschungsdatenzentrum Qualiservice] (o.J.): Helpdesk. Downloads. <https://www.qualiservice.org/de/helpdesk.html#downloads>. Letzter Zugriff: 16.07.2023.
- forschungsdaten.info (2023a): Forschung und Daten managen. Willkommen auf der Informationsplattform forschungsdaten.info! <https://forschungsdaten.info/>. Letzter Zugriff: 16.07.2023.
- forschungsdaten.info (2023b): Der Datenmanagementplan: Eine Wegbeschreibung für Daten. <https://forschungsdaten.info/themen/informieren-und-planen/datenmanagementplan/>. Letzter Zugriff: 16.07.2023.
- forschungsdaten.info (2023c): Datensicherheit und Backup. <https://forschungsdaten.info/themen/speichern-und-rechnen/datensicherheit-und-backup/>. Letzter Zugriff: 18.07.2023.
- Franken, Lina (2022): Digitale Methoden für qualitative Forschung. Computationelle Daten und Verfahren (UTB Studium). Münster: Waxmann.
- Golla, Sebastian J., Henning Hofmann & Matthias Bäcker (2018): Connecting the Dots. Sozialwissenschaftliche Forschung in Sozialen Online-Medien im Lichte von DSGVO und BDSG-neu. In: Datenschutz und Datensicherheit 42, 89–100. <https://doi.org/10.1007/s11623-018-0900-x>.
- Heibges, Maren, Frauke Mörike & Markus A. Feufel (2019): Wann braucht Ethnografie eine Einverständniserklärung? Praktische Antworten auf ethische Fragen zu ethnografischen Methoden in der HCI-Forschung. In: Mensch und Computer 2019 – Workshopband, Bonn 2019. <https://doi.org/10.18420/muc2019-ws-258-02>.
- Huber, Elisabeth & Sabine Imeri (2021): Informed Consent in Ethnographic Research: A Common Practice Facing New Challenges. Qualiservice Working Paper 4. <https://doi.org/10.26092/elib/1070>.
- Humboldt-Universität zu Berlin (2022): Dateien strukturieren. Empfehlungen zur Verzeichnisstruktur und Dateibenennung. <https://www.cms.hu-berlin.de/de/dl/dataman/arbeiten/sichern/dateistruktur>. Letzter Zugriff: 18.07.2023.

- Humboldt-Universität zu Berlin (2023): Datenmanagementplan. Anleitung zur Erstellung eines Datenmanagementplans (DMP). https://www.cms.hu-berlin.de/de/dl/dataman/arbeiten/dmp_erstellen. Letzter Zugriff: 16.07.2023.
- Imeri, Sabine (2018): Ordnen, archivieren, teilen. Forschungsdaten in den ethnologischen Fächern. In: Österreichische Zeitschrift für Volkskunde LXXII/121, Heft 2/ 201, 213–243. <https://resolver.obvsg.at/urn:nbn:at:at-ubi:4-5937>.
- Imeri, Sabine & Elisabeth Huber (2023): Strukturieren, Dokumentieren, (Ab)Sichern. Effekte von Forschungsdatenmanagement in der ethnografischen Forschung. In: Hamburger Journal für Kulturanthropologie 16, 85–104. <http://nbn-resolving.de/urn:nbn:de:gbv:18-8-20771>.
- Imeri, Sabine & Michaela Rizzolli (2022): CARE Principles for Indigenous Data Governance: Eine Leitlinie für ethische Fragen im Umgang mit Forschungsdaten? In: O-Bib. Das Offene Bibliotheksjournal 9/2, 1–14. <https://doi.org/10.5282/o-bib/5815>.
- Inhorn, Marcia C. (2004): Privacy, Privatization, and the Politics of Patronage: Ethnographic Challenges to Penetrating the Secret World of Middle Eastern, Hospital-Based in vitro Fertilization. In: Social Science & Medicine 59/10, 2095–2108.
- Kindling, Maxi & Peter Schirmbacher (2013): „Die digitale Forschungswelt“ als Gegenstand der Forschung: Lehrstuhl Informationsmanagement 64/2-3, 127–136. <https://doi.org/10.1515/iwp-2013-0017>.
- Kretzer, Susanne (2013): Arbeitspapier zur Konzeptentwicklung der Anonymisierung /Pseudonymisierung in Qualiservice. <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-47605-2>.
- Kretzer, Susanne, Kati Mozygemba, Jan-Ocko Heuer & Elisabeth Huber (2020): Erläuterungen zur Verwendung der von Qualiservice bereitgestellten Vorlagen für die informierte Einwilligung. In: Qualiservice Working Papers, 2. Bremen: Forschungsdatenzentrum Qualiservice. <https://doi.org/10.26092/elib/192>.
- Meyermann, Alexia & Maike Porzelt (2014): Hinweise zur Anonymisierung qualitativer Daten. Version 1.1. fdbinfo, 1. Frankfurt am Main: Leibniz-Institut für Bildungsforschung und Bildungsinformation (DIPF). <https://doi.org/10.25656/01:21968>.
- Meyermann, Alexia & Maike Porzelt (2019): Datenschutzrechtliche Anforderungen in der empirischen Bildungsforschung. Eine Handreichung. Version 2.1. fdbinfo, 6. Frankfurt am Main: Leibniz-Institut für Bildungsforschung und Bildungsinformation (DIPF). <https://doi.org/10.25656/01:21990>.
- Mozygemba, Kati & Betina Hollstein (2023): Anonymisierung und Pseudonymisierung qualitativer textbasierter Forschungsdaten – eine Handreichung. In: Qualiservice Working Papers, 5. Bremen: Forschungsdatenzentrum Qualiservice. <https://doi.org/10.26092/elib/2525>.
- Murphy, Alexandra K., Colin Jerolmack & DeAnna Smith (2021): Ethnography, Data Transparency, and the Information Age. In: Annual Review of Sociology 47/1, 41–61.
- Nicolai, Tom, Kati Mozygemba, Susanne Kretzer & Hollstein, Betina (2021): QualiAnon - Qualiservice Tool for Anonymizing Text Data (version 1.0.1). Qualiservice. University of Bremen. <https://github.com/pangaea-data-publisher/qualianon>.
- Poirier, Lindsay, Kim Fortun, Brandon Costelloe-Kuehn & Mike Fortun (2020): Metadata, Digital Infrastructure, and the Data Ideologies of Cultural Anthropology. In: J. W. Crowder, Mike Fortun, Rachel Besara & Lindsay Poirier (Hgs.), Anthropological Data in the Digital Age. New Possibilities – New Challenges. Cham: Palgrave Macmillan, 209–237. https://doi.org/10.1007/978-3-030-24925-0_10.

- RatSWD [Rat für Sozial- und Wirtschaftsdaten] (2020): Handreichung Datenschutz. 2. vollständig überarbeitete Auflage. RatSWD Output 8/6. <https://doi.org/10.17620/02671.50>.
- RatSWD [Rat für Sozial- und Wirtschaftsdaten] (2023): Forschungsdatenmanagement in kleinen Forschungsprojekten - Eine Handreichung für die Praxis. (RatSWD Output 7/3). <https://doi.org/10.17620/02671.72>.
- Rizzolli, Michaela, Sabine Imeri & Elisabeth Huber (2023) (im Erscheinen): Ethnografische Forschungsmaterialien zur Archivierung und Nachnutzung vorbereiten und dokumentieren – ein Überblick für Forschende. In: Qualiservice Working Papers. Bremen: Forschungsdatenzentrum Qualiservice.
- Scheper-Hughes, Nancy (2000): Ire in Ireland. In: *Ethnography* 1/1, 117–140.
- Shklovski, Irina & Janet Vertesi (2013): Un-Googleing Publications. The Ethics and Problems of Anonymization. In: CHI'13 Extended Abstracts on Human Factors in Computing Systems, 2169–2178. ACM Digital Library. <https://doi.org/10.1145/2468356.2468737>.
- SIEF [Société Internationale d'Ethnologie et de Folklore] (2019): Statement on Data Management. https://www.siefhome.org/downloads/publications/statements/SIEF_Statement%20Data%20Management.pdf. Letzter Zugriff: 14.07.2023.
- Unger, Hella von (2014): Forschungsethik in der qualitativen Forschung. Grundsätze, Debatten und offene Fragen. In: Hella von Unger, Petra Narimani & Rosaline M'Bayo (Hgs.), *Forschungsethik in der qualitativen Forschung. Reflexivität, Perspektiven, Positionen*. Wiesbaden: Springer VS, 15–39.
- Van den Hoonard, Will C. (2004): Fostering Human Dignity. Some Inherent Ethical Dimensions of Qualitative Research. In: Jurij Fikfak, Frane Adam & Detlef Garz (Hgs.), *Qualitative Research. Different perspectives, emerging trends*. Založba: ZRC, 265–279.
- VerbundFDB [Verbund Forschungsdaten Bildung] (2015): Checkliste zur Erstellung eines Datenmanagementplans in der empirischen Bildungsforschung. Version 1.1. fdb info, 2. Frankfurt am Main: Leibniz-Institut für Bildungsforschung und Bildungsinformation (DIPF). <https://doi.org/10.25656/01:22298>.
- VerbundFDB (2018a): Formulierungsbeispiele für „informierte Einwilligungen“. Version 2.1. fdb info, 4. Frankfurt am Main: Leibniz-Institut für Bildungsforschung und Bildungsinformation (DIPF). <https://doi.org/10.25656/01:22301>.
- VerbundFDB (2018b): Formulierungsbeispiele für „informierte Einwilligungen“ in leichter Sprache. Version 1.1. fdb info, 5. Frankfurt am Main: Leibniz-Institut für Bildungsforschung und Bildungsinformation (DIPF). <https://doi.org/10.25656/01:22302>.
- VerbundFDB (2018c): Dateien benennen und organisieren. <https://www.forschungsdaten-bildung.de/dateien-benennen#bvd>. Letzter Zugriff: 16.07.2023.
- Virtuelles Datenschutzbüro (o.J.): Gesetze und Verordnungen. <https://www.datenschutz.de/home/gesetze-und-verordnungen/>. Letzter Zugriff: 16.07.2023.
- Wilkinson, Mark D. et al. (2016): The FAIR guiding principles for scientific data management and stewardship. *Scientific Data*, 3 (160018). <https://doi.org/10.1038/sdata.2016.18>.

Autor:inneninformation

Sabine Imeri ist wissenschaftliche Mitarbeiterin des Fachinformationsdienstes Sozial- und Kulturanthropologie (FID SKA) an der Universitätsbibliothek der Humboldt-Universität zu

Berlin und dem Forschungsdatenzentrum Qualiservice an der Universität Bremen. Mit einem fachlichen Hintergrund in Europäischer Ethnologie hat sie mit Blick auf die Archivierung und Nachnutzung ethnografischer Daten Bedarfserhebungen durchgeführt und Anforderungsprofile entwickelt. Sie beschäftigt sich dabei auch mit ethischen Fragen, insbesondere des Forschungsdatenmanagements ethnografischer Daten, aber auch im Kontext von (Retro-)Digitalisierung und Open Access. Darüber hinaus vertritt sie den FID SKA im Bereich FDM in zahlreichen Arbeitsgruppen, etwa der Konsortien der Nationalen Forschungsdateninfrastruktur (NDFI) oder der ethnologischen Fachgesellschaften.

Martina Klausner ist Professorin für Digitale Anthropologie und Science and Technology Studies am Institut für Kulturanthropologie und Europäische Ethnologie an der Goethe-Universität Frankfurt. Als Anthropologin mit einem besonderen Schwerpunkt im Bereich der Science and Technology Studies bilden ihre Forschungsthemen ein Spektrum aktueller gesellschaftlicher Phänomene ab: Digitalisierungs- und Datafizierungsprozesse von/in Stadt; die Veränderungen von politischer Beteiligung durch online-Plattformen und Daten-Aktivismus sowie die Regulierung von neuen digitalen Technologien und Verfahren, wie Künstlicher Intelligenz. Neben den thematischen Schwerpunkten sind in ihren Arbeiten vor allem auch methodologische Fragen zentral, wie der Einsatz digitaler Methoden für ethnografische Forschung.

Michaela Rizzolli ist wissenschaftliche Mitarbeiterin am Forschungsdatenzentrum Qualiservice an der Universität Bremen. Mit einem fachlichen Hintergrund in Europäischer Ethnologie beschäftigt sie sich dort schwerpunktmäßig mit der Entwicklung passender Workflows und Tools für die Archivierung von ethnografischen Forschungsdaten und fungiert als Ansprechperson für fachspezifische Fragen rund um die Archivierung von Forschungsmaterial aus den ethnologischen Fächern. Zu ihren weiteren Tätigkeitsfeldern gehört die Antragsberatung von Forschenden hinsichtlich des Umgangs mit Forschungsdaten sowie die Konzeption und Durchführung von Workshops zu FDM-Themen wie z.B. zu Archivierung und Bereitstellung, Informierter Einwilligung und Anonymisierung/Pseudonymisierung.