LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
PROF. DR. HELLA VON UNGER
INSTITUT FÜR SOZIOLOGIE
LEHRBEREICH QUALITATIVE METHODEN DER EMPIRISCHEN SOZIALFORSCHUNG

Datenmanagement in der qualitativen Methodenausbildung

Handreichung für Studierende

Diese Handreichung enthält Vorschläge zum Umgang mit qualitativen Daten, die von Studierenden im Rahmen ihrer Methodenausbildung erhoben und ausgewertet werden. Was ist zu beachten, um einen verantwortungsvollen Umgang mit diesen Daten zu ermöglichen? Welche Rolle spielen forschungsethische und datenschutzrechtliche Aspekte? Diese Fragen stehen im Zentrum der Vorschläge, die wir hier auf Basis unserer Erfahrungen am Institut für Soziologie der LMU München zusammengetragen haben.

Die Handreichung richtet sich an Studierende und bezieht sich auf qualitative Daten, die in digitaler Form vorliegen. Die Handreichung deckt bei weitem nicht alle Fragen und Eventualitäten des qualitativen Datenmanagements ab. Zum einen entwickeln sich die technischen Möglichkeiten der digitalen Kommunikation, Vernetzung und Datenbearbeitung ständig weiter und auch datenschutzrechtliche Bestimmungen und deren Auslegung ändern sich. Zum anderen lässt sich das Datenmanagement in der qualitativen Forschung grundsätzlich nur begrenzt vorab planen. Die tatsächlich passende Form eines verantwortungsvollen Umgangs mit den Daten wird i.d.R. sukzessive und gemeinsam mit den Dozierenden/Projektverantwortlichen im Forschungsprozess ausgearbeitet. Wir möchten Studierende also ermuntern, den Dialog mit den Dozierenden zu diesen Fragen immer wieder zu suchen. Dabei – so unsere Hoffnung – können diese Hinweise Orientierung und Anregungen bieten. Vorschläge zur Verbesserung dieser Handreichung nehmen wir gerne entgegen (unger@lmu.de).

Inhalt

1 Allgemeines zur Datensicherheit: LMU-Emails und Infrastruktur nutzen

Bitte nutzen Sie aus datenschutzrechtlichen Gründen grundsätzlich Ihre LMU-E-Mail und die digitale Infrastruktur der Universität.

Bitte schalten Sie ggf. die Weiterleitungsfunktion, mit der E-Mails automatisch von Ihrer LMU-Email (@campus.lmu.de) an eine private E-Mail-Adresse weitergeleitet werden, für den Zeitraum der qualitativen Forschungsarbeit aus.
Da in der qualitativen Forschung oft mit sensiblen Daten gearbeitet wird, ist eine Nutzung privater E-Mail-Konten nicht empfehlenswert. Die Zugriffs- und Speicherbedingungen kommerzieller E-Mail-Anbieter (wie web.de, outlook, googlemail etc.), entsprechen nicht akademischen Standards von Datensicherheit und Vertraulichkeit. Daher nutzen Sie bitte grundsätzlich Ihre LMU-Email.

Bitte speichern Sie Daten an sicheren Orten, d.h. auf *passwortgeschützten* Laptops, Computer und Festplatten sowie universitären Online-Speichern wie LMU-Teams oder Synch&Share (s.u.).

1.1 Selbst Daten erheben in der qualitativen Methodenausbildung

Am Institut für Soziologie der LMU findet die qualitative Methodenausbildung in verschiedenen Formaten statt. In Übungen, Seminaren und Forschungspraktika haben Sie Gelegenheit, praktische Forschungskompetenzen *hands-on* zu erwerben. Dabei erheben Sie auch oft eigene Daten und werten diese aus.

Qualitative Forschung lebt von der Reflexion und Diskussion der eigenen Beobachtungen und Interpretationen. Der Austausch mit anderen Forscher*innen (z.B. im Rahmen von Interpretationsgruppen und Forschungswerkstätten) spielt eine zentrale Rolle. Daher arbeiten Sie auch in der Methodenausbildung in der Regel in Arbeitsgruppen zusammen (2-4 Personen).

In manchen Lehrveranstaltungen arbeiten die Arbeitsgruppen jeweils dezentral mit einem eigenen Datenkorpus. In anderen Seminaren arbeiten alle zusammen an einem Thema und das ganze Seminar greift auf einen gemeinsamen Datenkorpus zu. In beiden Fällen werden Daten geteilt (*data sharing*).

1.2 *Data-sharing* über LMU Teams

Als technische Infrastruktur für ein sicheres *data sharing* hat sich „LMU Teams“ bewährt, die auf universitätseigenen Servern ein hohes Maß an Sicherheit und Datenschutz und zugleich eine gute Zugänglichkeit der Daten für Lehrforschungszwecke gewährleisten.[1]

LMU-Teams werden über ein einfaches Formular[2] beantragt. Teams für das gesamte Seminar werden von den Dozierenden beantragt. Studierende können für ihre Arbeitsgruppen aber auch eigene Teams beantragen. Dazu geben Sie auf dem Formular „Ich möchte ein LMU-Team gründen“[3] das „Studierenden-Team“ als Team-Form an.

[1] Bei *LMU Teams* gibt es verschiedene Teamarten: der „Virtuelle Seminarraum“ eignet sich insb. für Lehrveranstaltungen; zudem gibt es „Projektgruppen“ und „Studierendenteams“, die auch von Studierenden eingerichtet werden können; http://www.hilfe.teams.uni-muenchen.de (Zugriff: 01.02.2022).
[2] http://www.hilfe.teams.uni-muenchen.de/gruenden/antrag/index.html (Zugriff: 01.02.2022).
[3] https://www.hilfe.teams.uni-muenchen.de/gruenden/registrierung/index.html (Zugriff: 01.02.2022)

Um LMU Teams nutzen zu können, ist es erforderlich, dass Ihre Benutzerkennung über das LMU-Portal freigeschaltet ist.[4] In den Teams können dann verschiedene Ordner (und Unterordner) angelegt werden, z.B. für Literatur, Folien, Daten und Memos. Die Teams können auch für Diskussionen, Chats, Fragen und Termine/Kalenderfunktionen genutzt werden.

Auch der LRZ-Dienst „Sync & Share", der allen Mitarbeitenden und Studierenden der Münchner Universitäten zur Verfügung steht, hat sich bewährt.[5]

2 Vertraulichkeit im Umgang mit den Daten

2.1 Vertraulichkeitsvereinbarung (im Seminar)

Ein zentraler Grundsatz im Umgang mit den Daten ist Vertraulichkeit. Bitte fragen Sie Ihre Dozierenden, wenn Ihnen nicht ganz klar ist, was das in einem konkreten Fall bedeutet.

Viele Dozierende treffen mündliche oder auch schriftliche Vereinbarungen mit Studierenden zum Thema „Vertraulichkeit". Ein Beispiel für eine schriftliche Vertraulichkeitsvereinbarung finden Sie im Anhang). Diese Vereinbarung wird zwischen Dozierenden und Studierenden getroffen - sie ist von einer Einverständniserklärung der Studienteilnehmenden zu unterscheiden (s.u.).

2.2 Kontaktdaten und Feldzugang

Bei der Planung des Feldzugangs stellen sich praktische, datenschutzrechtliche, forschungsethische und technische Fragen im Umgang mit den Daten. Kontaktdaten von (potentiellen) Studienteilnehmer*innen (z.B. Namen, Adressen, Telefonnummern, E-Mail-Adressen) sind besonders vertraulich zu behandeln, sorgsam (und getrennt von den anderen Daten) aufzubewahren und i.d.R. nach Projektende zu löschen. Sind weitere Kontaktaufnahmen geplant (z.B. im Rahmen einer Panelstudie), sollte dies zu Beginn klar kommuniziert und ein explizites Einverständnis der Teilnehmenden eingeholt werden (vgl. 2.3).

Auch aus methodischen und analytischen Gründen empfiehlt es sich, den Feldzugang gut zu dokumentieren. Falls dieser über soziale Netzwerke, Plattformen, Chats oder E-Mails hergestellt wird, sind auch diese Interaktionen als Daten zu speichern und vertraulich zu behandeln. Bereits hier ist unbedingt auf die Sicherheit der Kommunikationswege zu achten. Dazu gehört wie erwähnt, dass Sie nur Ihre **universitäre E-Mail** verwenden, Weiterleitungsfunktionen an andere, private E-Mails deaktivieren, sowie ggf. verschlüsselte Kommunikationswege in Betracht ziehen (siehe 2.8 zu Verschlüsselung).

2.3 Informierte Einwilligung

In der Regel ist für empirische Sozialforschung eine informierte Einwilligung der Teilnehmenden erforderlich. Diese kann mündlich oder schriftlich eingeholt werden (vgl. unsere Handreichung zu Studieninformation und informierter Einwilligung).

Falls das Einverständnis der Teilnehmenden mündlich eingeholt wird, ist es ratsam, dies zu dokumentieren (z.B. in Feldnotizen, Postskripten oder auf Audioaufzeichnungen).

[4] http://www.hilfe.teams.uni-muenchen.de/beitreten/kennung_freischalten/index.html (Zugriff: 01.02.2022)
[5] https://syncandshare.lrz.de/login (Zugriff: 01.02.2022); vergleiche auch Fußnote 11.

Nehmen Sie sich in der Lehrveranstaltung Zeit – und fragen Sie nach - um das Vorgehen mit den anderen Studierenden in Ihrer Gruppe und den Dozierenden zu klären. Fragen Sie, ob Sie das Einverständnis schriftlich oder mündlich einholen sollen, und ob es eine Vorlage gibt.

Falls das Einverständnis der Teilnehmenden schriftlich eingeholt wird, fragen Sie nach, welches Formular Sie ggf. nutzen sollen – oder ob Sie selbst eins entwickeln. Klären Sie auch, wo und wie die unterzeichneten Einverständniserklärungen aufbewahrt werden – ob Sie das übernehmen oder die Dozierenden diese zentral verwahren wollen. Muster für schriftliche Einverständniserklärungen finden sich z.B. bei RatSWD (2014), Helfferich (2009) und Audiotranskription[6].

Es gibt begründete Ausnahmen von der Regel, eine informierte Einwilligung einzuholen (z.B. bei Feldforschung an öffentlichen Plätzen oder bei der Analyse von frei im Internet zugänglichen Dokumenten).

2.4 Gespräche aufzeichnen

Bitte achten Sie darauf, bei Audioaufzeichnungen von Interviews und Gruppengesprächen (und gleiches gilt für Videoaufzeichnungen) nur professionelle Aufnahmegeräte zu verwenden.

Audioaufnahmegeräte können am Institut für Soziologie gegen eine Kaution für drei Monate ausgeliehen werden.[7]

Wir raten dringend davon ab, private Smartphones als Aufnahmegeräte zu verwenden. Zwar verfügen diese mittlerweile über leistungsstarke Aufnahmemöglichkeiten, allerdings sind private Smartphones oft vielfältig vernetzt und es besteht die Gefahr, dass die Aufnahmen (aus Versehen oder automatisch) z.B. in Cloud-Dienste hochgeladen werden, wo sie nicht länger ausreichend geschützt, sondern möglicherweise für Dritte zugänglich sind - oder gar formal zum Eigentum der Anbieter werden.

Bitte löschen Sie die Daten (nach der Übertragung auf einen sicheren Speicherort) wieder vollständig von dem Aufnahmegerät. Es empfiehlt sich, die Löschung auf dem Stick des Aufnahmegeräts am Computer vorzunehmen – und anschließend auf der Anzeige des Aufnahmegeräts nochmal zu überprüfen, ob die Löschung auch tatsächlich geklappt hat.

2.5 Daten aufbereiten und benennen

In der qualitativen Forschung wird vielfältiges empirisches Material gesammelt, so dass sich Fragen nach einer sinnvollen Aufbereitung, Benennung und Sicherung dieser Daten stellen. Nicht alle Daten lassen sich digital aufbereiten. Grundsätzlich ist es sinnvoll, sich frühzeitig auf eine Benennungspraxis zu einigen, um eine möglichst einheitliche Bezeichnungspraxis zu etablieren. Dies erleichtert das Datenmanagement und fördert die Übersicht über den Datenkorpus (vgl. Tab. 1 für ein Beispiel).

[6] Ein Muster für eine Einwilligungserklärung für Interviews, die der neuen EU-Datenschutzverordnung entspricht, findet sich bei: https://www.audiotranskription.de/qualitative-Interviews-DSGVO-konform-aufnehmen-und-verarbeiten (Zugriff: 01.02.2022).

[7] https://www.soziologie.uni-muenchen.de/institut/it-service1/software_geraete_verleih1/index.html (Zugriff: 01.02.2022)

Datensorte	Formel	Beispiel
Feldnotizen	FN_Name Studierende_Datum/JJMMTT	FN_Rösch_180525
Audiofiles	INT_ID/Pseudonym_INT Datum	INT_Lara_180530
Transkripte	TS_ID/Pseudonym_INT Datum	TS_Lara_180530
Postskripte	PS_ID/Pseudonym_Datum	PS_Lara_180530
Dokumente	Autor*in/Org_Jahr_Titelstichwort	DAH_2015_Jahresbericht
Zeitungsartikel	Zeitung_Datum_Titelbegin	SZ_180530_Roseanne Twitter

Tab. 1 Beispiel für die Bezeichnung von ausgewählten Datensorten *(Anmerkung zur Legende: Feldnotizen (FN) werden hier nach den Verfasser/innen benannt; Audioaufzeichnungen von Interviews (INT) dagegen nach dem Code (ID) der Interviews und dem Pseudonym der Interview-Partner*innen; auch die Bezeichnung der Postskripte (PS) verweist auf den/die Interviewte*n, und nicht auf den/die Interviewer*in und Verfasser*in).*

Bei einem gemeinsamen, zentral verwalteten Datenkorpus, der Interviews enthält, empfiehlt es sich, frühzeitig gemeinsam einen Transkriptionsstil (mit entsprechender Zeichen-Legende) zu wählen und diesen konsistent anzuwenden.[8] Ähnliches gilt für die Aufbereitung von Videodaten.

2.6 Daten anonymisieren und pseudonymisieren

Grundsätzlich werden Daten möglichst frühzeitig anonymisiert, um die Teilnehmenden zu schützen. Dabei kommen unterschiedliche Anonymisierungsstrategien zur Anwendung (vgl. Saunders et al. 2015). Gebräuchlich ist die Pseudonymisierung von Namen (z.B. Lara statt Birgit oder Herr Huber statt Herr Strubel). Auch weitere Namen (z.B. von Organisationen) sowie weitere Informationen zu Personen und Orten werden gelöscht, verändert oder vergröbert (z.B. kann „München" zu einer „süddeutschen Großstadt" vergröbert werden; aus einer „Geschäftsführerin" wird eine „Angestellte in leitender Funktion", etc.). Sinn und Zweck ist es, die Identifikation der beteiligten Personen zu verhindern und letztere zu schützen. Allerdings sind qualitative Daten in der Regel so beschaffen, dass sie nur unter Verlusten ihrer Aussagekraft und im Grunde niemals vollständig anonymisiert werden können (es sei denn sie werden komplett geschwärzt). „Insider" können Personen allein daran erkennen, wie sie sprechen und was sie sagen. Daher reicht die formale Anonymisierung oft nicht aus, um Rückschlüsse auf Personen auszuschließen. Gleichzeitig müssen wir vorsichtig sein, nicht zu viel zu löschen oder zu verändern, um unsere Daten noch sinnvoll auswerten zu können.

Praktische Tipps zur Anonymisierung:

- **Die Grundregel lautet: so wenig wie möglich, und so stark wie nötig zu anonymisieren**. So wenig wie möglich, um so viel der Aussagekraft wie möglich beizubehalten, aber so viel wie nötig in dem Sinne, dass bei erhöhten Risiken und absehbarem Schaden stärkere Eingriffe zum Schutz der Teilnehmenden erforderlich sein können;

- Die Anonymisierung erfolgt in mehreren Schritten: das Rohmaterial der Daten wird zunächst bei der Aufbereitung der Daten (möglichst sparsam) anonymisiert; nach der Analyse werden zitierte Ausschnitte aus dem Material beim Verfassen der Hausarbeiten oder Publikationen ggf. stärker anonymisiert;

- Im **Rohmaterial** also zunächst eher zurückhaltend anonymisieren (d.h. zunächst nur Personennamen pseudonymisieren), um Bezüge und Details und damit die

[8] Vgl. die Hinweise zur Transkription bei Dresing/Pehl auf www.audiotranskription.de (Zugriff: 01.02.2022).

Aussagekraft der Daten zu erhalten und eine gehaltvolle interpretative Analyse zu ermöglichen;

- Im Verlauf der Analyse und insbesondere bei **Zitaten in der Hausarbeit** (ähnlich wie bei Forschungsberichten und Publikationen) wird aufwendiger anonymisiert und am Material entschieden, welche weitere Form der Anonymisierung angemessen ist; hierbei gilt es, abzuwägen, welche Informationen notwendigerweise erhalten bzw. (an dieser Stelle) aufgeführt werden müssen, um den Kontext zu beschreiben und Verstehen zu ermöglichen, und welche Informationen gekürzt, ausgelassen oder vergröbert (oder getrennt dargestellt) werden müssen, um ausreichenden Schutz zu gewährleisten, z.B. weil die Daten sensibel, die Personen besonders verletzbar oder die Themen brisant sind.

In einem Lehrforschungsprojekt mit Geflüchteten (von Unger 2017) wurde beispielsweise sehr aufwendig und umfassend anonymisiert, weil die Teilnehmenden aufgrund ihrer aktuellen Situation und ihres Fluchthintergrunds in sozialer, rechtlicher und ökonomischer Hinsicht sehr vulnerabel waren. In anderen Studien kann dagegen weniger Schutz erforderlich sein, weil die Personen weniger verletzlich oder die Daten weniger sensibel sind.

Genauso können sich, je nach Forschungsinteresse und Umständen, neue und andere Fragen ergeben (wie beispielsweise besondere Regelungen zum Schutz von Minderjährigen). Es wird grundsätzlich empfohlen, bei Unsicherheiten die Dozierenden zu fragen sowie den Austausch in der Arbeitsgruppe zu suchen.

Falls Übersetzungen anfallen, sind die Übersetzer*innen und Dolmetscher*innen bezüglich der Anonymisierung, Vertraulichkeit und einem insgesamt angemessenen Umgang mit den Daten zu verpflichten.

2.7 Data-Sharing – für alle Datensorten?

In den Lehrveranstaltungen werden die Daten unter Studierenden und mit den Dozierenden geteilt. Dozierende sollten gemeinsam mit den Studierenden entscheiden, welche Daten im Seminar geteilt werden. Zum Beispiel sind **Feldnotizen** nicht nur sehr schwer und aufwendig zu anonymisieren, sondern können zudem sehr persönlich sein und viel über die Person der Forscherin/des Forschers Preis geben – daher sollten die jeweiligen Verfasser*innen mitentscheiden, welche Daten in der Lehrveranstaltung den anderen Studierenden zur Verfügung gestellt werden (und welche nicht).

Eine weitere Frage ist es, ob Audiodateien geteilt werden sollen, da diese deutlich sensibler und noch schwerer zu anonymisieren sind, da Stimmen erkannt werden können. Wir handhaben den Zugang zu dieser Datensorte am Lehrbereich meist eher restriktiv. In dem o.g. Lehrforschungsprojekt mit jungen, geflüchteten Interviewpartner*innen haben wir beispielsweise die Transskripte und Postskripte der verwertbaren Interviews über ein LMU Team zur Verfügung gestellt, nicht jedoch die Feldnotizen oder Audiofiles. Feldnotizen wurden in den Arbeitsgruppen besprochen und teilweise gegenseitig gelesen, aber als vollständige Rohdaten, wenn überhaupt, nur innerhalb der Kleingruppen geteilt. Die Audiodateien der Interviews (die im ersten Semester erhoben und transkribiert wurden), wurden (im zweiten Semester) nicht über das gemeinsame LMU Team zur Verfügung gestellt. Für den Fall, dass Audiodateien nachgehört werden mussten, z.B. um Transkripte nachzubessern, haben wir die Audiodateien an institutseigenen Computern in einem geschützten Ordner auf dem Server des Instituts *ad personam* zugänglich gemacht (auf dem CIP Laufwerk)[9].

[9] Zur Einrichtung sicherer CIP-Laufwerke siehe die Hinweise des IT Support des Instituts für Soziologie: https://dienste.soziologie.uni-muenchen.de/faq-pmwiki/pmwiki.php?n=Main.InfosFuerLehrende (Zugriff: 01.02.2022)

Bei der technischen Umsetzung des *data sharing* im Seminar liegt ein besonderes Augenmerk auf der Sicherheit der Daten. Wie bereits erwähnt raten wir dazu, eine sichere, universitätseigene Infrastruktur zu nutzen. Bei LMU Teams ist der Zugang auf die subskribierten Personen begrenzt. Es können Dokumente hoch- und heruntergeladen und auf eigenen Rechnern gespeichert werden. Falls dies vorgesehen ist, sollten die Daten-Dokumente zusätzlich noch mittels eines Passworts verschlüsselt werden, damit sie bei einem Download auf private Rechner weiterhin geschützt bleiben (auch Word-Dokumente lassen sich verschlüsseln).[10]

Die Dozierenden benötigen in der Regel einen Nachweis für erbrachte Prüfungsleistungen und bekommen alle erhobenen Daten oder zumindest Einsicht in diese Daten.

Bei Lehrveranstaltungen mit einem **zentralen** Datenkorpus, stellen sie den Datenkorpus auf Basis der Einreichungen der Studierenden zusammen, überprüfen die Daten z.B. auf ausreichende Anonymisierung und passen Datei-Bezeichnungen u.ä. an.

Für Lehrforschungsprojekte, in denen das Datenmanagement **dezentral** von mehreren Arbeitsgruppen durchgeführt wird, und in denen das data sharing auf die Mitglieder dieser Gruppen begrenzt bleibt, lohnt es sich, den Modus der Datenspeicherung und des Zugangs zu besprechen. Bitte nutzen Sie keine externen Anbieter wie Dropbox, Google Drive oder vergleichbare Angebote, da die Forschungsdaten hier nicht sicher sind. Falls Sie kein eigenes LMU-Team beantragen möchten, können sie auf **LMU Sync & Share**[11] als weiteren LMU-Dienst ausweichen oder auf andere Möglichkeiten, etwa verschlüsselte und eigene kontrollierbare Server.

2.8 Verschlüsselung von Daten und Kommunikation

Dateien, Ordner, Speichermedien und Kommunikation (z.B. E-Mails oder Chats) lassen sich potentiell verschlüsseln oder mit einem Passwort schützen.

PDFs und Word-Dokumente lassen sich über die Software mit einem Passwort schützen[12].

Auch ganze Ordner lassen sich als ZIP-Ordner, also als komprimierter Ordner, verschlüsseln[13]. Allerdings verschwindet hier der Passwortschutz, sobald die einzelnen Dateien wieder entpackt werden.

Speichermedien, z.B. USB-Sticks oder Festplatten, lassen sich ebenso verschlüsseln. Laufwerke lassen sich z.B. über das Programm Bitlocker, welches in Windows integriert ist schützen[14]. Sensible Daten werden nur auf geschützten Speichermedien gespeichert und genutzt.

Auch E-Mail-Kommunikation ist verschlüsselbar. Voraussetzungen dafür sind eine E-Mail-Adresse, die per POP3 oder IMAP zugänglich ist (die LMU-Adressen sind es) und die Nut-

[10] Hinweis: Passwortgeschützte Daten lassen sich allerdings nicht mit allen Programmen zur datengestützten Analyse weiter nutzen – MAXQDA kann beispielsweise keine passwortgeschützten Dateien öffnen.

[11] Sync & Share funktioniert wie andere Cloud-Dienste, z-B. Dropbox. Dort können nach Anmeldung Ordner erstellt werden und dieser für bestimmte Personen über die Nutzerkennung bereitgestellt werden. Es stehen jedem 50GB Speicher zur Verfügung. Zusätzlich gibt es einen Client für alle Betriebssysteme, sowie eine App für Apple und Android. Es lassen sich Personen über die E-Mailadresse zum Ordner einladen.

[12] Die genaue Anleitung findet sich unter den FAQs des IT Support des Instituts für Soziologie https://dienste.soziologie.uni-muenchen.de/faq-pmwiki/pmwiki.php?n=Main.PDF-Passwortschutz (Zugriff: 01.02.2022)

[13] Bei der Erstellung eines ZIP Ordners mit dem Programm IZArc (z.B. über Rechtsklick auf einen Ordner > Add to ZIP-File Archive) gibt es die Option „Encryption". Dort AES 256 bit auswählen und ein Passwort festlegen)

[14] Z.B. über Rechtsklick auf den Wechseldatenträger und die Option „Bitlocker aktivieren" lässt sich sehr schnell ein USB Stick schützen.

zung eines Email-Clients (etwa Thunderbird).[15] Zur doppelten Sicherheit gibt es bei der LMU ein gesondertes Zertifizierungsverfahren, welches befolgt werden muss, um über LMU Email-Adressen verschlüsselt zu kommunizieren.[16]

Weitere Tipps

- Anonymisierung nachhaltig gewährleisten: Qualitative Rohdaten grundsätzlich nicht oder nur nach gründlicher Abwägung und mit expliziter Einwilligung der Teilnehmer*innen für Dritte zugänglich machen, um die Privatsphäre der Teilnehmenden zu schützen und die Chancen einer Dechiffrierung der Anonymisierung zu begrenzen; niemals die ganzen Rohdaten veröffentlichen, sondern nur in Auszügen zitieren;[17]

- Bei der Einreichung von Prüfungsleistungen klären, ob, wie und in welcher Form die Rohdaten den Dozierenden zur Verfügung gestellt werden (z.B. nicht im Anhang, sondern gesondert über passwortgeschützte Sticks, s.u.).

3 Nach der Prüfungsleistung

3.1 Löschung der Rohdaten

Am Lehrbereich für qualitative Methoden (Prof. von Unger) raten wir davon ab, bei der Abgabe von Prüfungsleistungen qualitative Rohdaten (z.B. Feldnotizen, Transkripte) als Anhang mit einzureichen, da diese Daten wie erwähnt nicht komplett bzw. nur mit unverhältnismäßig hohem Aufwand anonymisierbar sind und die langfristige Aufbewahrung der Prüfungsleistungen sich der Kontrolle der Dozierenden entzieht (Prüfungsleistungen werden vom Institut zentral archiviert; BA- und MA-Arbeiten auch vom Prüfungsamt). Es ist allerdings möglich, die Rohdaten **gesondert,** z.B. auf einem Datenträger einzureichen, der zurückgegeben oder zerstört wird, wenn die Prüfungsleistung erbracht, die Hausarbeit besprochen und das Projekt abgeschlossen wird.

Bitte fragen Sie bei Ihren Dozierenden nach, wie Sie mit den Rohdaten verfahren sollen.

Mit dem offiziellen Projektende stellt sich die Frage nach der Löschung bzw. weiteren Verwendung der Daten. Hier sind entsprechende datenschutzrechtliche Vorgaben zu beachten. Wir legen in der Regel in der Vertraulichkeitserklärung mit den Studierenden einen Zeitpunkt für die Löschung von privaten Kopien auf Speichergeräten der Studierenden fest (z.B. Semesterende, Datum der Abgabe der Hausarbeit oder Ende des Lehrforschungsprojekts). Sollten Studierende ihre Daten für das Verfassen einer Abschlussarbeit weiterverwenden, ist es ratsam eine gesonderte Regelung zu treffen.[18]

[15] Online finden sich sehr viele Anleitungen und Tutorials zur Verschlüsselung von Emails, siehe etwa https://netzpolitik.org/2013/anleitung-so-verschlusselt-ihr-eure-e-mails-mit-pgp/ (Zugriff: 01.02.2022)
[16] Die genaue Anleitung findet sich unter den FAQs des IT Support des Instituts für Soziologie https://dienste.soziologie.uni-muenchen.de/faq-pmwiki/pmwiki.php?n=Main.MailverschlSselung (Zugriff: 01.02.2022)
[17] Zur Debatte um die digitale Archivierung qualitativer Daten zu (Sekundär-) Forschungszwecken siehe: https://www.ratswd.de/dl/RatSWD_WP_267.pdf (Zugriff: 01.02.2022).
[18] Gesonderte Hinweise zum Löschen von Daten siehe unter anderem: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html (Zugriff: 01.02.2022).

3.2 Sekundäranalysen

Sie haben Lust auf mehr – und wollen die Forschungsarbeit weiterverfolgen, z.B. im Rahmen einer BA- oder MA-Arbeit?
Dann nehmen Sie frühzeitig Kontakt a) mit der möglichen Betreuungsperson auf, und b) klären Sie mit den Dozierenden der Lehrveranstaltung, ob Sie die Daten aus der Lehrveranstaltung weiter nutzen dürfen, und wenn ja, welche und wie. Dies ist grundsätzlich nur nach Rücksprache möglich. Dabei sind nicht nur die Persönlichkeitsrechte der beforschten Personen, sondern auch die der Kommilliton*innen zu beachten.

3.3 Anmerkungen zu rechtlichen Rahmenbedingungen – DSGVO

Die seit dem 25.Mai 2018 gültigen EU-weiten Regelungen zur Datenschutzgrundverordnung (DSGVO)[19] betreffen auch das Datenmanagement in der qualitativen Sozialforschung. Was das praktisch bedeutet, wird aktuell geklärt. Wir werden bei der nächsten Aktualisierung dieser Handreichung diesen Punkt stärker ausführen.

Es ist in jedem Fall empfehlenswert, das **Datenmanagement** für den gesamten Prozess von der Datenerhebung bis zum Löschen der Daten zu **dokumentieren**. Für Lehrforschungsprojekte ist es hierbei auch von Bedeutung, welche Personen Zugriff auf die entsprechenden Daten haben.

4 Literatur und Links

Berliner Methodentreffen (2007): Memorandum für eine fundierte Methodenausbildung in den Human- und Sozialwissenschaften. https://berliner-methodentreffen.de/weiteres-memorandum/ (Zugriff: 01.02.2022).

DGS und BDS (2017): Ethik-Kodex der Deutschen Gesellschaft für Soziologie (DGS) und des Berufsverbands Deutscher Soziologen (BDS). https://soziologie.de/dgs/ethik/ethik-kodex (Zugriff: 01.02.2022).

Helfferich, Cornelia (2009): Die Qualität qualitativer Daten. Manual für die Durchführung qualitativer Interviews. Wiesbaden: VS Verlag.

Hopf, Christel (2009): Forschungsethik und qualitative Forschung. In: Flick, Uwe; von Kardoff, Ernst; Steinke, Ines (Hg.): Qualitative Forschung. Ein Handbuch. Reinbek bei Hamburg: Rowohlt, S.589–600.

RatSWD (2014): Datenschutzrechtliche Anforderungen bei der Generierung und Archivierung qualitativer Interviewdaten. Working Paper 238. Rat für Sozial- und Wirtschaftsdaten, Berlin. http://www.ratswd.de/dl/RatSWD_WP_238.pdf (Zugriff: 01.02.2022).

RatSWD (2015): Archivierung und Sekundärnutzung von Daten der qualitativen Sozialforschung. Eine Stellungnahme des RatSWD. Rat für Sozial- und Wirtschaftsdaten, Berlin. https://www.ratswd.de/dl/RatSWD_Output1_Qualidaten.pdf (Zugriff: 01.02.2022).

RatSWD (2016): Forschungsdatenmanagement in den Sozial-, Verhaltens- und Wirtschaftswissenschaften. Orientierungshilfen für die Beantragung und Begutachtung datengenerierender und datennutzender Forschungsprojekte. RatSWD Output 3 (5). Rat für Sozial- und Wirtschaftsdaten, Berlin. https://www.ratswd.de/dl/RatSWD_Output3_Forschungsdatenmanagement.pdf (Zugriff: 01.02.2022).

[19] https://www.datenschutz-grundverordnung.eu/ (Zugriff: 01.02.2022).

Schaar, Katrin (2017): Die informierte Einwilligung als Voraussetzung für die (Nach-) Nutzung von Forschungsdaten. RatSWD Working Paper 264. https://www.ratswd.de/dl/RatSWD_WP_264.pdf (Zugriff: 01.02.2022).

Saunders, Benjamin; Kitzinger, Jenny; Kitzinger, Celina (2015): Anonymising Interview Data: Challenging and compromise in practice. *Qualitative Research*, 15 (5), S.616-632.

von Unger, Hella (2014a): Forschungsethik in der qualitativen Forschung: Grundsätze, Debatten und offene Fragen. In: von Unger, Hella; Narimani, Petra; M'Bayo, Rosaline (Hg.) Forschungsethik in der qualitativen Forschung: Reflexivität, Perspektiven, Positionen. Wiesbaden: Springer VS, S.15-39.

von Unger, Hella (2014b): Forschungsethik in der Methodenlehre: Erfahrungen aus einem Soziologie-Seminar. In: von Unger, Hella; Narimani, Petra; M'Bayo, Rosaline (Hg.): Forschungsethik in der qualitativen Forschung: Reflexivität, Perspektiven, Positionen. Wiesbaden: Springer VS, S.209-231.

von Unger, Hella (Hg.) (2017): Junge Geflüchtete, Bildung und Arbeitsmarkt. Ein Lehrforschungsprojekt. München: LMU München. http://nbn-resolving.de/urn:nbn:de:bvb:19-epub-41306-4 (Zugriff: 01.02.2022).

von Unger, Hella (2018): Forschungsethik, digitale Archivierung und biographische Interviews. In Lutz, Helma; Schiebel, Martina Schiebel; Tuider, Elisabeth (Hg.): Handbuch Biographieforschung. Wiesbaden: Springer VS, S.681-693.

von Unger, Hella; Narimani, Petra; M'Bayo, Rosaline (Hg.) (2014): Forschungsethik in der qualitativen Forschung. Reflexivität, Perspektiven, Positionen. Wiesbaden: Springer VS.

Weitere Links und Hinweise finden Sie auf der Webseite des Lehr- und Forschungsbereichs qualitative Methoden der empirischen Sozialforschung: http://www.qualitative-sozialforschung.soziologie.uni-muenchen.de unter „Ressourcen".

Danksagung

Zu dieser Handreichung (bzw. einer Vorläufer-Version) haben Mitarbeiter*innen des Lehrbereichs für qualitativen Methoden der empirischen Sozialforschung am Institut für Soziologie der LMU München wesentlich beigetragen. Dazu gehören u.a. Yvonne Berger, Gözde Celik, Oskar Fischer, Holger Knothe, Dimitra Kostimpas, Anne Götz, Anna Huber, Dennis Odukoya, Hans Pongratz, Viktoria Rösch, Penelope Scott und Jana Türk. Vielen Dank!

Stand: 01.02.2022

5 Anhang

5.1 Beispiel Vertraulichkeitsvereinbarung mit Studierenden

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

INSTITUT FÜR SOZIOLOGIE
PROF. DR. HELLA VON UNGER
LEHRBEREICH FÜR QUALITATIVE METHODEN DER EMPIRISCHEN SOZIALFORSCHUNG

Vertraulichkeitsvereinbarung

Name:	Matrikel-Nr.:	Dozent/in: Prof. Dr. Hella von Unger

Hiermit verpflichte ich mich, alle im Rahmen der Veranstaltung „Junge Geflüchtete, Bildung und Arbeitsmarkt" (Master Forschungspraktikum, 6 SWS, 15232, WiSe 2016/2017) erhobenen und zur Verfügung gestellten Daten streng vertraulich zu behandeln.

Das heißt:

- Ich verwende personenbezogene Daten und Informationen ausschließlich in anonymisierter Form, so dass kein Rückschluss auf die Identität der Teilnehmenden möglich ist (entsprechend dem Bundesdatenschutzgesetz und dem Bayrischen Datenschutzgesetz; s.u.).
- Ich verwahre die Daten an einem sicheren und passwortgeschützten Ort.
- Ich übergebe alle Daten (z.B. Audioaufzeichnungen, anonymisierte Transkripte und Feldnotizen) mit meiner Hausarbeit dem Lehrbereich für Qualitative Methoden (Prof. von Unger).
- Ich verwende zur Sicherung/Lagerung der Daten keine Online-Dienste wie Dropbox, Google Drive oder sonstige Clouds (mit Ausnahme LRZ Sync+Share und LMU TEAMS)
- Ich vernichte private Kopien der Daten (digital und ausgedruckt) zum Ende des Wintersemesters (23.4.2017).
- Ich verwende die Daten nur nach Rücksprache und mit ausdrücklicher Genehmigung von Prof. von Unger für weitere wissenschaftliche Arbeiten (z.B. Master-Arbeiten).
- Ich werde keine die Daten betreffenden Informationen schriftlich oder mündlich an dritte Personen, die nicht an der Lehrveranstaltung teilnehmen, weitergeben oder zugänglich machen.
- Ich gehe achtsam mit den Daten im öffentlichen Raum um (z.B. Gespräche in der U-Bahn)

Ich habe den Ethik-Kodex der Deutschen Gesellschaft für Soziologie (DGS) zur Kenntnis genommen (http://www.soziologie.de/de/die-dgs/ethik-kommission/ethik-kodex.html).
Bei Fragen wende ich mich an eine/n Mitarbeiter/in des Lehrbereichs für qualitative Methoden der empirischen Sozialforschung oder an Prof. von Unger (unger@lmu.de).

Ort, Datum: Unterschrift:

5.2 Check-Liste zum Datenmanagement in der qualitativen Methodenlehre

Zusammenfassend schlagen wir vor, folgende Punkte beim Datenmanagement zu beachten:

- ✓ Campus-Email nutzen (und automatische Weiterleitung ausschalten)?
- ✓ Sichere digitale Infrastruktur für *data sharing* (z.B. LMU-Teams) nutzen
- ✓ Fragen zu Vertraulichkeit geklärt?
- ✓ Fragen zu Studieninformation, Kontaktdaten und Feldzugang besprochen?
- ✓ Informierte Einwilligung (der Teilnehmenden) – mündlich oder schriftlich?
- ✓ Professionelle Aufnahmegeräte verwenden
- ✓ Jegliche digitale Forschungskommunikation nur über LMU-Campus-Emails
- ✓ Anonymisierungsstrategien besprechen
- ✓ Passwort- Schutz der Daten (Verschlüsselung)
- ✓ Speicherorte (z.B. externe Festplatten oder USB-Sticks) verschlüsseln
- ✓ Sichere, universitätseigene Cloud-Dienste für Gruppenarbeiten einrichten
- ✓ Aufbereitung (z.B. Bezeichnung, Transkriptionslegende) der Daten klären
- ✓ Einreichung, Aufbewahrung und Löschung der Rohdaten klären (z.B. Aufzeichnungen auf Aufnahmegeräten vor Rückgabe löschen)
- ✓ Möglichkeiten der Weiter- und Wiederverwendung der Daten (z.B. für Publikationen oder Qualifikationsarbeiten) absprechen
- ✓ Datenmanagement dokumentieren