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 Dozierende

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 dabei forschungsethische und datenschutzrechtliche Aspekte? Diese Fragen stehen im Zentrum der Vorschläge, die wir auf Basis unserer Erfahrungen am Institut für Soziologie der LMU München zusammengetragen haben.

Die Handreichung richtet sich an Dozierende und bezieht sich auf qualitative Daten, die in digitaler Form vorliegen. Die Struktur der Handreichung spiegelt die zeitliche Abfolge der Planung, Umsetzung und Nachbereitung einer Lehrveranstaltung. Sie enthält zudem eine Liste mit weiterführender Literatur, ein Beispiel für eine Vertraulichkeitsvereinbarung (mit Studierenden) sowie eine Checkliste.

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. Auch datenschutzrechtliche Bestimmungen ändern sich (vgl. neue EU-DSGVO, S.9). Zum anderen lässt sich das Datenmanagement in der qualitativen Forschung grundsätzlich nur begrenzt vorab planen. Die tatsächlich passende Form des Datenmanagements wird i.d.R. sukzessive und gemeinsam mit den Studierenden im Forschungsprozess ausgearbeitet. Wir möchten Dozierende also ermuntern, den Dialog mit den Studierenden zu diesen Fragen zu suchen, denn Studierende kennen sich auch in technischen Fragen oft sehr gut aus. Wir hoffen, dass diese Hinweise hilfreiche Anregungen bieten. Vorschläge zur Verbesserung und Aktualisierung nehmen wir gerne entgegen (unger@lmu.de).

Inhalt

1 Vorbereitung der Lehrveranstaltung

Lehrveranstaltungen, in denen Studierende praktische Erfahrungen in der qualitativen Forschung sammeln, erstrecken sich idealerweise über zwei Semester, um ausreichend Zeit für die Entwicklung einer Fragestellung und die sorgfältige Erhebung, Aufbereitung und Auswertung der Daten vorzusehen. Bei einsemestrigen Veranstaltungen muss man in der Regel Abstriche machen oder besondere Vorbereitungen treffen (z.B. kann man eine Fragestellung vorgeben, den Feldzugang für die Studierenden bereits im Vorfeld organisieren, auf zeitaufwendige Verfahren der Datenerhebung, -aufbereitung und Auswertung verzichten oder mit bereits vorliegenden Daten arbeiten). Wir gehen nachfolgend davon aus, dass Studierende als Primärforschende selbst Daten erheben.

1.1 Planung

Am Institut für Soziologie der LMU nehmen i.d.R. jeweils zwischen 20-30 Studierende an den praktisch ausgerichteten Lehrveranstaltungen der qualitativen Methodenausbildung teil (z.B. Übungen, Seminare, Forschungspraktika). Es empfiehlt sich, bereits bei der Planung (und im Seminarplan) ausreichend Zeit für Fragen des Datenmanagements und damit verbundene Themen wie die informierte Einwilligung, Vertraulichkeit und Anonymisierung vorzusehen, um einen verantwortungsvollen Umgang mit den Daten zu fördern.

Grundsätzlich unterscheiden wir zwischen Lehrveranstaltungen, in denen Kleingruppen[1] jeweils dezentral mit einem eigenen Datenkorpus arbeiten (a), und Lehrforschung, in der das ganze Seminar auf einen gemeinsamen Datenkorpus zugreift (b). In beiden Fällen werden Daten unter den Studierenden geteilt (*data sharing*). Im Falle eines (von allen geteilten) zentralen Datenkorpus liegt die Verantwortung für und die Koordination des Datenmanagements meist stärker bei den Dozierenden als bei der dezentralen Variante.

1.2 Bereitstellung einer sicheren Infrastruktur für *data sharing*

Als technische Infrastruktur für ein sicheres *data sharing* hat sich die Plattform „LMU Teams“ bewährt, die auf universitätseigenen Servern ein hohes Maß an Sicherheit und Datenschutz und zugleich eine gute Zugänglichkeit der Daten für Lehrveranstaltungen gewährleistet.[2] **LMU-Teams** werden (i.d.R. von Dozierenden oder Tutor*innen) über ein einfaches Formular[3] beantragt. Es können ein oder mehrere Administrator*innen und Teamleiter*innen bestimmt werden. Sobald die Studierenden ihre Benutzerkennung über das LMU-Portal freigeschaltet haben[4], kann die Teamleitung sie namentlich für das LMU-Team subskribieren. In den Teams können dann verschiedene Ordner (und Unterordner) angelegt werden, z.B. für Literatur, Folien und Daten. Die Teams können auch für Diskussionen, Fragen und Termine/Kalenderfunktionen genutzt werden. Für die Arbeitsgruppen der Studierenden können hier Ordner eingerichtet werden. Alternativ können die Studierenden auch ein eigenes LMU-Team für ihre Zusammenarbeit beantragen, um untereinander Daten, Memos und ähnliches auszutauschen.

---

[1] Wir präferieren das Format der Gruppenarbeit für die Erhebung und Auswertung qualitativer Daten, um den Austausch und die gegenseitige Unterstützung unter den Studierenden zu befördern und das gemeinsame Forschen und Interpretieren bereits in der Ausbildung zu üben (vgl. Memorandum des Berliner Methodentreffens (2007)). Hausarbeiten werden jedoch teilweise auch als Einzelarbeiten verfasst.

[2] 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: 30.05.2018).

[3] http://www.hilfe.teams.uni-muenchen.de/gruenden/antrag/index.html (Zugriff: 30.05.2018).

[4] http://www.hilfe.teams.uni-muenchen.de/beitreten/kennung_freischalten/index.html (Zugriff: 13.06.2018)

Auch der LRZ-Dienst „Sync & Share“, der allen Mitarbeitenden und Studierenden der Münchner Universitäten zur Verfügung steht, hat sich sehr bewährt.[5] Kolleg*innen an anderen Fakultäten der LMU haben zudem mit der Lernplattform „Moodle“ gute Erfahrungen gemacht.

Anmerkung: Wird mit externen Partner*innen zusammengearbeitet, die ebenfalls Zugang zu den Daten benötigen, muss für diese ein extra Zugang beantragt werden.[6] Oder Sie nutzen andere Lösungen des *data sharing*, wie z.B. den CIP-Server oder portable, lokale Speicher, wie externe Festplatten o.ä., auf denen die Daten dann verschlüsselt werden sollten (s.u.).

2 Umsetzung der Lehrveranstaltung

Es hat sich bewährt, Studierenden immer wieder die Gelegenheit zu geben, Fragen zu praktischen Aspekten des Umgangs mit den Daten und zum Datenschutz (inklusive rechtlicher Vorgaben und ihrer Interpretation und Umsetzung im jeweiligen Projektkontext) zu klären. Zusätzlich bietet es sich an auf die Online-Dienste der LMU zu verweisen, wie etwa LMU Teams, oder LMU Sync & Share. Die Erfahrung hat gezeigt, dass viele Studierende diese Angebote (noch) nicht kennen.

2.1 Vertraulichkeitsvereinbarung (mit den Studierenden)

Ein zentraler Grundsatz im Umgang mit den Daten ist Vertraulichkeit. Es hat sich als hilfreich erwiesen, Vertraulichkeit wiederholt zu thematisieren und mit Beispielen zu veranschaulichen, was einen vertraulichen Umgang auszeichnet – und was nicht. Zudem kann Vertraulichkeit auch durch eine mündliche oder schriftliche Vereinbarung mit den Studierenden verbindlich gemacht werden (ein Beispiel einer Vertraulichkeitsvereinbarung finden Sie im Anhang). Diese Vereinbarung wird zwischen Dozierenden und Studierenden getroffen. Sie ist von einer Einverständniserklärung der Studienteilnehmenden zu unterscheiden (siehe unten).

2.2 Kontaktdaten und Feldzugang

Bei der Planung des Feldzugangs stellen sich 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 ggf. 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.

Es empfiehlt 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 sollten Studierende darauf aufmerksam gemacht werden auf die Sicherheit der Kommunikationswege zu achten. Dazu gehört beispielsweise nur ihre **universitäre E-Mail** für die forschungsbezogenen Kommunikation zu verwenden (und Weiterleitungen an andere, private E-Mails für den Zeitraum der Forschung zu deaktivieren) sowie ggf. verschlüsselte Kommunikationswege in Betracht zu ziehen (siehe Kapitel 2.8 zu Verschlüsselung).

[5] https://syncandshare.lrz.de/login (Zugriff: 3.7.2018); vergleiche auch Fußnote 13.
[6] Für Hinweise zu externen Zugängen zu LMU Teams siehe: https://www.hilfe.teams.uni-muenchen.de/faq/externe/index.html (Zugriff: 3.7.2018).

2.3 Informierte Einwilligung

Viele Studierende wissen bereits, dass Studienteilnehmer*innen grundsätzlich über die Forschung und den Umgang mit den Daten informiert werden sollen.[7] Oft bestehen jedoch Unsicherheiten hinsichtlich der Frage, **welche** Informationen, sowie **wann** und **wie** diese kommuniziert werden sollten. Hier gibt es keine Patentlösung, sondern es sind maßgeschneiderte, projektspezifische Lösungen gefragt, die den beteiligten Personen, Kommunikationsformen, Erkenntniszielen und Vorgehensweisen entsprechen. 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 mündlich eingeholt wird, ist es ratsam, dies zu dokumentieren (z.B. in Feldnotizen, Postskripten oder auf Audioaufzeichnungen). Nehmen Sie sich ausreichend Zeit, um das Vorgehen mit den Studierenden im Kurs zu besprechen. Stellen Sie evtl. eine Einverständniserklärung bereit und sammeln Sie die unterschriebenen Exemplare ein, um diese sicher aufzubewahren (insb. bei Lehrforschungsprojekten mit einem zentralen Datenkorpus). Muster für schriftliche Einverständniserklärungen finden sich z.B. bei RatSWD (2014) und Helfferich (2009).[8]

2.4 Gespräche aufzeichnen

Bei der Audioaufzeichnung von Interviews (und gleiches gilt für Videoaufzeichnungen) sollte darauf geachtet werden, dass Studierende professionelle Aufnahmegeräte verwenden. Audioaufnahmegeräte können am Institut für Soziologie gegen eine Kaution für drei Monate ausgeliehen werden.[9] **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. Es hat sich bewährt, Studierende explizit darauf anzusprechen und dies ausführlich zu begründen.

Bitte erinnern Sie die Studierenden auch daran, die **Daten von den Aufnahmegeräten** nach der Übertragung auf einen sicheren Speicherort wieder **vollständig zu löschen.** 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.

---

[7] Allerdings denken manche Studierende, sie sollten die Teilnehmenden besser nicht vorab informieren, um sozial erwünschte Reaktionen zu vermeiden und ‚realistischere' („unverzerrte") Daten zu bekommen (vgl. Unger 2014b: 220). Es lohnt sich also nachzufragen und nicht nur forschungsethische Prinzipien und datenschutzrechtliche Auflagen zu klären, sondern auch methodologische und erkenntnistheoretische Grundlagen der qualitativen Forschung zu besprechen. Selbstverständlich gibt es auch begründete Ausnahmen von der Regel, eine informierte Einwilligung einzuholen (z.B. bei Feldforschung an öffentlichen Plätzen) – und auch diese gilt es ggf. entsprechend nachvollziehbar zu machen.

[8] Ein weiteres 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: 3.7.2018); vgl. auch die kritischen Hinweise dazu auf der Mailingliste für qualitative Forschung im Juni 2018; http://www.qualitative-forschung.de/mailingliste/index.html (Zugriff: 3.7.2018).

[9] Weitere Informationen zu Programm- und Geräteverleih auf der Homepage des IT-Service des IfS https://www.soziologie.uni-muenchen.de/institut/it-service1/software-geraeteverleih1/index.html (Zugriff: 2.7.2018)

2.5 Daten aufbereiten und benennen

In der qualitativen Forschung wird vielfältiges empirisches Material gesammelt, was zur Folge hat, 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 mit den Studierenden auf eine Benennungspraxis zu einigen, um eine möglichst einheitliche Bezeichnungspraxis zu etablieren. Dies erleichtert das Datenmanagement und fördert die Übersicht über den Datenkorpus.

Datensorte	**Formel**	**Beispiel**
Feldnotizen	FN_Name Studierende_Datum/JJMMTT	FN_Rösch_180525
Audiofiles von Interviews	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-Format für die Bezeichnung von ausgewählten Datensorten

Bei einem gemeinsamen, zentral verwalteten Datenkorpus, der Interviews enthält, empfiehlt es sich, frühzeitig mit den Studierenden einen Transkriptionsstil (mit entsprechender Zeichen-Legende) zu wählen, und diesen konsistent anzuwenden.[10] 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 können unterschiedlichen Anonymisierungsstrategien zur Anwendung kommen (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 ggf. 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. „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.

Praktische Tipps zur Anonymisierung:

- **Grundregel*: so wenig wie möglich, und so stark wie nötig 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;

[10] Vgl. die Hinweise zur Transkription bei Dresing/Pehl auf www.audiotranskription.de (Zugriff:13.6.2018]

- Die Anonymisierung erfolgt oft in mehreren Schritten; das Rohmaterial der Daten wird dabei grundsätzlich weniger stark anonymisiert als zitierte Ausschnitte in Publikationen;

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

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

2.7 Data-Sharing

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 können **Feldnotizen** nicht nur sehr schwer und aufwendig zu anonymisieren, sondern zudem sehr persönlich sein und viel über die Person der Forscherin/des Forschers Preis geben – daher sollten die Studierenden mitentscheiden können, 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. Daher handhaben wir den Zugang zu dieser Datensorte meist eher restriktiv. In dem o.g. Lehrforschungsprojekt mit jungen, geflüchteten Interviewpartner*innen haben wir beispielsweise die Transskripte und Postskripte der verwertbaren Interviews über das LMU Team zur Verfügung gestellt, nicht jedoch die Feldnotizen oder Audiofiles. Feldnotizen wurden in den Kleingruppen besprochen und teilweise gegenseitig gelesen, aber als vollständige Rohdaten, wenn überhaupt, dann 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)[11].

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,

[11] 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: 2.7.2018)

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).[12]

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. Dabei sollten die Studierenden daran erinnert werden, keine externen Anbieter wie Dropbox, Google Drive oder vergleichbare Angebote zu nutzen, da die Forschungsdaten hier nicht sicher sind. Falls die Studierenden kein eigenes LMU-Team beantragen möchten, können sie auf **LMU Sync & Share**[13] 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[14].

Auch ganze Ordner lassen sich als ZIP-Ordner, also als komprimierter Ordner, verschlüsseln[15]. 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[16]. Die Dozierenden könnten die Studierenden darauf hinweisen, etwa sensible Daten lediglich auf geschützten Speichermedien zu speichern und zu nutzen.

---

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

[13] 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.

[14] 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: 14.11.2017)

[15] 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)

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

Auch E-Mail-Kommunikation ist verschlüsselbar. Voraussetzungen dafür ist eine E-Mail-Adresse, die per POP3 oder IMAP zugänglich ist (die LMU-Adressen sind es) und die Nutzung eines Email-Clients (etwa Thunderbird).[17] Zur doppelten Sicherheit gibt es bei der LMU ein gesondertes Zertifizierungsverfahren, welches befolgt werden muss um über LMU Email-Adressen verschlüsselt zu kommunizieren.[18]

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;[19]

- Bei der Einreichung der Rohdaten durch die Studierenden empfehlen wir darauf zu achten, dass universitätsinterne Kommunikationswege (z.B. Campus-E-Mail) und Speichermöglichkeiten (LRZ) genutzt werden.

3 Nachbereitung der Lehrveranstaltung

3.1 Löschung der Rohdaten

Wir raten 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). 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.

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.[20]

3.2 Sekundäranalysen

Studierenden kann – je nach Absprache – die Möglichkeit eingeräumt werden, die Daten nach Beendigung des Lehrforschungsprojekts weiter zu nutzen (bspw. im Rahmen von Qualifizierungsarbeiten). Hier muss darauf geachtet werden, nicht nur die Persönlichkeitsrechte der beforschten Personen, sondern auch der Kommiliton*innen zu schützen.

[17] 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: 11.9.2017)
[18] 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: 14.11.2017)
[19] Zur Debatte um die digitale Archivierung qualitativer Daten zu (Sekundär-) Forschungszwecken siehe: https://www.ratswd.de/dl/RatSWD_Output1_Qualidaten.pdf (Zugriff: 13.6.2018).
[20] Gesonderte Hinweise zum Löschen von Daten siehe unter anderem: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/richtigloeschen_node.html (Zugriff: 13.06.2018).

Auch die Frage der Urheber*innenschaft sollte bedacht werden (d.h. die Zustimmung der jeweiligen Primärforschenden, die die Daten erhoben haben, ist möglicherweise erforderlich).[21]

3.3 Anmerkungen zu rechtlichen Rahmenbedingungen – DSGVO

Die seit dem 25.Mai 2018 gültigen EU-weiten Regelungen zur Datenschutzgrundverordnung (DSGVO)[22] betreffen auch das Datenmanagement in der qualitativen Sozialforschung. Was das praktisch bedeutet, ist zu diesem Zeitpunkt allerdings noch nicht ganz klar. Wir hoffen, bei der nächsten Aktualisierung der Handreichung zu diesem Punkt mehr sagen zu können.

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. http://www.qualitative-forschung.de/methodentreffen/memorandum/index.html (Zugriff: 30.5.2018).

DGS (2017): Ethik-Kodex der Deutschen Gesellschaft für Soziologie (DGS) und des Berufsverbands Deutscher Soziologen (BDS). http://www.soziologie.de/de/die-dgs/ethik/ethik-kodex.html (Zugriff: 9.4.2018).

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: 8.7.2014). (*mit Vorlage für eine schriftliche Einverständniserklärung)

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: 13.06.2018).

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: 13.06.2018).

[21] Digitale Archivierung und Sekundäranalysen sind ein in der qualitativen Forschung kontrovers diskutiertes Thema, siehe dazu eine Diskussion auf dem Sozblog der Deutschen Gesellschaft für Soziologie: http://blog.soziologie.de/2015/08/qualitative-forschung-forschungsethik-streitpunkt-digitale-archivierung/ (Zugriff: 13.6.2018).

[22] https://www.datenschutz-grundverordnung.eu/ (Zugriff: 11.7.2018).

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: 13.06.2018).

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: 13.06.2018).

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/ressourcen/hinweise_qualitativ1/index.html

Danksagung

Zu dieser Handreichung haben mehrere Mitarbeiter*innen des Lehrbereichs für qualitativen Methoden der empirischen Sozialforschung am Institut für Soziologie der LMU München beigetragen, insbesondere Yvonne Berger, Holger Knothe, Dimitra Kostimpas, Dennis Odukoya, Hans Pongratz und Viktoria Rösch. Vielen Dank!

Stand: 11.7.2018

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:

- ✓ Genügend Zeit im Seminarplan eingeplant?
- ✓ Sichere digitale Infrastruktur für *data sharing* (z.B. LMU-Teams) bereitgestellt?
- ✓ Vertraulichkeit mit den Studierenden vereinbart? (mündlich oder schriftlich)
- ✓ Fragen zu Studieninformation, Kontaktdaten und Feldzugang besprochen?
- ✓ Informierte Einwilligung (der Teilnehmenden); ggf. schriftliche Einverständniserklärung
- ✓ Professionelle Aufnahmegeräte verwenden
- ✓ 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 der Studierenden
- ✓ Aufbereitung (z.B. Bezeichnung, Transkriptionslegende) der Daten frühzeitig 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