Datenschutzkonzept

Version 03, 20. März 2019

enthält: Verzeichnisse von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 und Abs. 2 DSGVO

Vorbemerkung

eLabour ist ein Forschungsdatenzentrum zur Archivierung und Bereitstellung von qualitativen Forschungsdaten der Arbeits- und Industriesoziologie (AIS). Die zugrundeliegenden Daten können einen erheblichen Schutzbedarf aus Datenschutzsicht erfordern, gleichzeitig können sie auch wichtige Beiträge zur Forschung und Wissenschaft ermöglichen. Die hierbei zugrunde liegenden Zielkonflikte angemessen aufzulösen ist eine wichtige Aufgabe von eLabour.

In diesem Dokument werden die Grundsätze zur sicheren Speicherung, Verarbeitung, Bereitstellung und Nutzung von qualitativen Forschungsdaten im Forschungsdatenzentrum eLabour dokumentiert und fortentwickelt. Das Datenschutzkonzept stellt den Ausgangspunkt der Dokumentation der Einhaltung datenschutzrechtlicher Verpflichtungen dar. Alle Abstrakten – also: nicht einzelfallbezogenen - Ausführungen zum Datenschutz liegen mit diesem Dokument inkl. seiner Anhängen gebündelt vor, oder sind darin mit Verweisen hinterlegt.

Dieses Datenschutzkonzept soll als „lebendiges Dokument“ regelmäßig vervollständigt und aktualisiert werden.

Es enthält derzeit neben einem einführenden Überblick,

- die Verfahrensdokumentation,
- Technische und organisatorischen Maßnahmen,
- Rollen- und Rechtekonzept und das
- Freigabekonzept.

Verträge und Vertragsvorlagen sowie Hinweise zur Durchführung von Datenschutzfolgeabschätzungen können ggf. im weiteren Projektverlauf ergänzt werden. Ebenso sollten spezifische Arbeitsanweisungen mit datenschutzrechtlichem Bezug in das Dokument aufgenommen werden.

Inhaltsverzeichnis

1. Einleitung: Das FDZ eLabour

Das Zentrum eLabour erschließt Daten aus qualitativen, empirischen Studien seit den 1970er Jahren mit IT-basierten Methoden und macht sie, wo möglich, für die weitere wissenschaftliche Nutzung nachhaltig verfügbar, um auf dieser Grundlage neue wissenschaftliche Fragestellungen auf Basis von Sekundäranalysen komplexer qualitativer Daten aus unterschiedlichen Studien zu ermöglichen. Hierzu wird eine geeignete Forschungsinfrastruktur, und Datenmanagement, sowie IT-basierte Anonymisierungs-, Such-, Annotations- und Analysetools kontinuierlich entwickelt, die den besonderen Anforderungen entsprechen, welche sich bei der Archivierung, Kuratierung und der Zugänglichmachung der qualitativen Daten aus der AIS für die wissenschaftliche Forschung ergeben.

Ziel des Forschungsdatenzentrums ist die dauerhafte Archivierung, Sicherung und weitere wissenschaftliche Nutzung von Forschungsdaten der AIS. Zugang und Verwendung dieser Forschungsdaten sind auf die wissenschaftliche Nutzung oder Lehre durch öffentlich geförderte WissenschaftlerInnen begrenzt. Um die wissenschaftliche Nachnutzung arbeitssoziologischer Forschungsdaten zu ermöglichen, werden umfangreiche empirische Studien der datengebenden Forschungsinstitute unter angemessener Berücksichtigung insbesondere von Vertraulichkeitsanforderungen aufbereitet und für wissenschaftliche Sekundäranalysen zur Verfügung gestellt.

Die Speicherung, Bereitstellung und Weitergabe qualitativer, sozialwissenschaftlicher Forschungsdaten stellt besondere Anforderungen an die Maßnahmen zum Datenschutz: Einerseits können qualitative Forschungsdaten aufgrund der prinzipiellen Offenheit der Erhebungsmethoden – auch sensible – personenbezogene Informationen enthalten, entsprechend müssen die Daten vor einer Weitergabe umfassend überprüft werden, um den Schutz sensibler, personenbezogener Informationen zu gewährleisten. Oft ist eine sinnvolle Nachnutzung und Analyse ohne personenbezogene Informationen nicht sinnvoll. Daher sind die Maßnahmen zum Datenschutz auch darauf ausgerichtet, die für eine weiter wissenschaftliche Nutzung notwendigen, personenbezogenen Informationen bis zu einem gewissen Grad zu erhalten oder risikomindernd zu umschreiben.

eLabour organisiert den Prozess der Speicherung, Aufbereitung und Bereitstellung der Forschungsdaten der beteiligten datenhaltenden Forschungseinrichtungen für die wissenschaftliche Nachnutzung.

Das Datenschutzkonzept umfasst die im Folgenden beschriebenen Bearbeitungsprozesse der

- Erstens: **Archivierung** von den Forschungseinrichtungen eingebrachten Forschungsdaten und
- zweitens, die **Übergabe** von Verwertungsrechten der datenhaltenden Einrichtungen an eLabour im Rahmen eines Freigabeprozesses.
- Drittens stellt eLabour diese Forschungsdaten für die wissenschaftliche Nachnutzung zur Verfügung, schließt Nutzungsverträge mit Wissenschaftlern ab und organisiert Beratung und Austausch bei der **Nutzung**.

Jenseits des Gegenstandes dieses Konzeptes ist der Schutz der Mitarbeiterdaten, etwa durch die im Rahmen des Prozesses entstehenden Protokollierungen.

2. Hintergrund: Warum werden welche personenbezogenen Daten archiviert?

Um wissenschaftlich und gesellschaftlich relevante Ergebnisse zur Entwicklung von Arbeit zu erzielen, umfasst arbeits- und organisationssoziologische Forschung die Erhebung und Analyse auch personenbezogener Informationen. Art und Umfang der Erhebung und Dokumentation personenbezogener Daten soll sich dabei auf das für die Forschungsziele Notwendige beschränken. Allerdings bewirkt die besondere Offenheit, Heterogenität und Gegenstandsbezogenheit qualitativer Forschung, dass solche Forschungsdaten jederzeit auch überraschende, sensible Informationen von und über Personen enthalten oder Rückschlüsse auf Personen und deren Handeln erlauben können.

Diese Forschungsdaten werden in wissenschaftlichen Forschungsprojekten mit Einwilligung der teilnehmenden Personen erhoben. Solche Einwilligungserklärungen enthalten üblicherweise die Zusicherung, dass die erhobenen Daten für dieses Forschungsprojekt anonymisiert verwendet werden. Aber wann aber ist eine Person nicht mehr identifizierbar, welche Informationen müssen hierzu entfernt werden? Denn neben den juristisch definierten personenbezogenen Daten enthalten qualitative Interviews und Beobachtungen oft auch für die ProbandInnen (und gelegentlich auch für InterviewerInnen) hochsensible Informationen mit zum Teil erheblichen wirtschaftlichen, sozialen und juristischen Schadensrisiken. Je offener die Methode, umso weniger absehbar ist die Wahrscheinlichkeit, dass solche sensiblen Informationen enthalten sind, d.h. es muss im Prinzip jedes Interview manuell darauf geprüft werden.

Nach der Weitergabe anonymisierter Daten an ein Archiv entfällt das Primärwissen über die teilnehmenden Personen aus der Erhebung, dennoch können Forschungsdaten aus der AIS systematisch Informationen enthalten, die eine Re-Identifikation von Personen ermöglichen und damit das Risiko, dass sensible Informationen zum Schaden der Person verwendet werden können. Hinzu kommt, dass die Einwilligungserklärungen oftmals (insbesondere bei zurückliegenden Studien) keine explizite Aussage zur der dauerhaften Archivierung und Verwendung in weiteren Forschungsprojekten enthalten, sodass die Weitergabe für andere Forschungsprojekte (i.d.R. Projekte mit ähnlichen Zielen wie die Primärforschung) durch die Einwilligung nicht abgedeckt ist.

Allerdings entspricht die Verwendung öffentlich finanzierter wissenschaftlicher Forschungsdaten für die weitergehende wissenschaftliche Forschung nach verbreiteter Ansicht (z.B. der öffentlichen Forschungsförderer und Wissenschaftsorganisationen) dem allgemeinen Interesse der Gesellschaft. Dem steht die gesetzliche und wissenschaftsethische Verpflichtung zum Schutz der personenbezogenen Daten bzw. der teilnehmenden Personen (und Organisationen) sowie das informationelle Selbstbestimmungsrecht der Personen entgegen.

Aus der methodischen Perspektive sind mit der Anonymisierung qualitativer Interviews besondere Herausforderungen verbunden: Erstens soll das Risiko der De-Anonymisierung untersuchter Person reduziert und kontrolliert werden, ganz beseitigen lässt es sich allerdings bei qualitativen Daten nicht. Insbesondere dann nicht, wenn eine sinnvolle Qualität der Daten für die wissenschaftliche Analyse gewährleistet werden soll. Aus der Perspektive wissenschaftlicher NutzerInnen von Forschungsdatenarchiven besteht ein grundsätzliches Interesse an Daten, die möglichst wenig verändert oder in ihrem Informationsgehalt möglichst wenig reduziert wurden. Je mehr die Originalforschungsdaten zum Schutz der Vertraulichkeit der Befragten anonymisiert wurden, desto geringer sind der analytische Gehalt der Daten und die entsprechenden Analysepotenziale für eine Sekundäranalyse. Umfassende Anonymisierungsmaßnahmen schränken die Nachnutzbarkeit von Forschungsdaten erheblich ein und reduzieren ihre Brauchbarkeit zur Beantwortung sekundäranalytischer Forschungsfragen.

Darüber hinaus sind organisationsbezogene Daten z.B. von Unternehmen sind schutzwürdig,

insbesondere auch aufgrund der schriftlichen oder mündlichen Absprachen der PrimärforscherInnen mit den beforschten Unternehmen. Letztere finden im Rahmen von Betriebsfallstudien generell statt und ihre Einhaltung ist sehr kritisch für die datenhaltenden Institute (Betriebszugang als Geschäftsgrundlage).

Die Anonymisierung beschränkt sich in der Arbeits- und Industriesoziologie entsprechend nicht nur auf Personen, sondern auch auf betriebliche und soziale Kontexte. Interviews in der AIS sind jedoch typischerweise in einen organisationalen Kontext eingebunden und finden oft am Arbeitsort statt. In den Interviews mit Beschäftigten eines bestimmten Betriebes geht es auch um deren subjektive Sicht auf betriebliche Probleme, auf Kollegen und Vorgesetzte, um soziale Beziehungen, Rollen und Konflikte. Solche Daten sind oft für betriebliche Insider und Personen mit Insiderinformationen sensibel und faktisch nicht anonymisierbar, daher muss durch strikte Zugangsbeschränkungen und Kontrollen verhindert werden, dass Insider Kenntnis von den Daten erlangen.

3. Forschungsdateninfrastruktur, Zwecke und Datenschutzmanagementprozess

Konkret umfasst die Forschungsdateninfrastruktur drei unterschiedliche Archive mit je eigenen Zugangsmöglichkeiten bzw. Prozessen:

Erstens, die nur für die jeweiligen Datenhalter zugänglichen Archive der Originaldaten (T1).

Zweites, ein Zwischenarchiv für die interne, gemeinsame Aufbereitung, Datenschutzbearbeitung und Kuratierung der Daten in eLabour (T2) mit striktem Rollen- und Rechtemanagement und Vertraulichkeitsverpflichtung für die Mitarbeitenden (siehe Rollen und Rechtemanagement in eLabour Anhang C).

Drittens das Forschungsdatenarchiv (T3), das den Zugang für WissenschaftlerInnen auf der Basis von Nutzungsverträgen ermöglicht. Vor der Übergabe der Daten in das dritte Archiv steht ein umfangreicher Datenschutzfolgeabschätzungs- und Freigabeprozess.

Erste Stufe: Ingest der Forschungsdaten vom Datenhalter

Vor dem Ingest sind die Einwilligungserklärungen der Primärstudie zu prüfen. Wenn die von den befragten Personen und Organisationen gegebenen Einwilligungserklärungen eine Archivierung und Sekundärnutzung explizit ausschließen (z.B. Zusicherung der Nutzung nur im Primärprojekt und anschließende Löschung), ist eine Archivierung und Sekundärnutzung der Originaldaten nicht möglich.

Die Nutzungs- und Verfügungsrechte an den Forschungsdaten liegen bis zur Freigabe bei den datenhaltenden Forschungsinstituten oder WissenschaftlerInnen. Diese sind weiterhin datenschutzrechtlich verantwortlich. Die datenhaltenden Institute tragen in dieser Phase die Verantwortung für die Einhaltung der von ihnen im Primärprojekt eingegangenen Verpflichtungen gegenüber den Betroffenen. Sie nutzen dafür die Infrastruktur, Dienste und Kompetenzen des FDZ.

Die technisch-organisatorischen Maßnahmen zum Datenschutz werden mit der Übertragung der Daten von eLabour im Auftrag der Datenhalter übernommen.

Insbesondere:

- die Speicherung sowie Backups erfolgen in verschlüsselter Form
- die Datenübertragung zur Bearbeitung der Daten erfolgt verschlüsselt
- Vergabe der Berechtigung für einen Zugriff auf die Daten erfolgt durch die Datenhalter

Die Forschungsdaten werden von den datenhaltenden Instituten in den ersten, internen Speicherbereich übertragen (T1), der exklusiv dem jeweiligen Datenhalter zur Verfügung gestellt wird. Die Daten werden hier als Backup und Langzeitsicherung in einer sicheren Umgebung so archiviert, dass die Verfügung und Verantwortung der Datenhalter transparent gewährleistet ist.

Im Weiteren werden sie im Auftrag des Datenhalters und in enger Zusammenarbeit in die Forschungsdateninfrastruktur des Zentrums eingelesen und dort gemeinsam aufbereitet. Hierfür werden IT-basierte "Anonymisierungs- und Freigabewerkzeuge" und geeignete Workflows für unterschiedliche Stufen und Anforderungen bereitgestellt.

Zweite Stufe: Kuratierung qualitativer Forschungsdaten

Die Originaldaten werden in einen gesicherten Speicherbereich zur Bearbeitung und Kuratierung übertragen und sicher gespeichert.

Informationen über das Einwilligungsverfahren der Primärforscher und ggf. vorhandene schriftliche oder mündliche Erklärungen sind sorgfältig zu dokumentieren und den Daten (im Ordner Studienbeschreibung und ggf. auf der Fallebene unter Fallerhebungsinstrumenten) beizufügen.

Im Datenschutzmanagement in eLabour durchläuft grundsätzlich jedes Dokument mit potentiell sensiblen personenbezogenen Daten, insbesondere alle empirischen Daten, eine interne Schadensfolgeabschätzung – von uns als Risikoanalyse bezeichnet. Diese führt zu einer abgestuften Freigabe zur Nutzung mit jeweils definierten technischen und organisatorischen Maßnahmen. Das eLabour-Datenschutzmanagement umfasst Verfahrensregeln, Praktiken und einen IT-gestützten Workflow für die Risikoklassifikation, Anonymisierung und Pseudonymisierung, sowie einen IT-basierten Freigabeprozess sowie Zugangsmöglichkeiten für WissenschaftlerInnen (Nutzende). Um der besonderen Sensibilität der qualitativen Daten gerecht zu werden, erfolgt ein differenzierter Freigabeprozess, in dem die Zugangsmöglichkeiten für wissenschaftliche NutzerInnen festgelegt werden. Auch diese können bis auf die Ebene einzelner Dokumente hinunter differenziert vergeben werden.

Die im Zuge der Anonymisierung und Pseudonymisierung entstehenden Dokumente (Schlüsseltabellen, Risikotabellen mit Klarnamen, Pseudonymen, sensiblen Daten) werden separat von den Forschungsdaten im gesicherten Archiv der Originaldaten (T1) gespeichert, auf den ausschließlich autorisierte Personen des Datengebers Zugriff haben, und im Zwischenspeicher gelöscht.

Im Folgenden wird der Prozess der datenschutzbezogenen Kuratierung qualitativer Forschungsdaten im Einzelnen beschrieben:

Im **ersten** Schritt erfolgt eine Risikoanalyse der Originalforschungsdaten, in der personenbezogene Informationen identifiziert und dokumentiert werden, sowie eine Abschätzung der möglichen Schadensfolgen für die TeilnehmerInnen der Primärstudie vorgenommen wird. Die formale Anonymisierung der TeilnehmerInnen (Klarnamen) wird überprüft und vervollständigt.

Dieser Schritt der Risikoanalyse erfolgt im optimalen Fall unmittelbar durch die Primärforschenden oder durch WissenschaftlerInnen des datenhaltenden Instituts, die die Daten sichten und aufbereiten. Grundlage sind die Originalforschungsdaten (wenn nicht datenschutzrechtliche oder andere Gründe aus Sicht des Datenhalters dagegensprechen.) Auf dieser Grundlage wird entschieden, ob und welche weiteren datenverändernden Maßnahmen zur Pseudonymisierung durchzuführen sind.

Ziel ist einerseits die Bewertung der Schadensrisiken für die untersuchten Personen und Organisationen, die entstehen würden, wenn der Inhalt der Dokumente mit der Person verknüpft (de-anonymisiert) und weitergegeben würde. Dabei kann unterschieden werden zwischen Beeinträchtigung organisationsinterner Beziehungen bzw. des unmittelbaren sozialen Nahbereichs der Person (bspw. Im Fall von Kritik an Kolleginnen und Kollegen oder an Vorgesetzten, Äußerungen

zum Lebenspartner, Sachbearbeiter), Beeinträchtigung der gesellschaftlichen und öffentlichen Stellung bzw. des "Ansehens" der Person (Medien, Öffentlichkeit), Beeinträchtigung der wirtschaftlichen Verhältnisse oder Sanktionen, etwa der Gefahr organisationaler Sanktionen (Bedrohung der ökonomischen „Existenz") oder gar der Gefahr staatlicher Sanktionen (Gefahr von Strafverfolgung).

Gleichzeitig wird das Risiko (bzw. die Wahrscheinlichkeit) einer Re-Identifikation bzw. De-Anonymisierung bewertet. Dieses Risiko kann anschließend durch datenverändernde Maßnahmen reduziert werden. Um den Grad des Schadensrisikos einzuschätzen, wird geprüft, sind welche Art von Schaden für die Befragten bei einer De-Anonymisierung schlimmstenfalls zu befürchten ist.

Außerdem wird eine Bewertung des Schadensrisikos für die Organisationen vorgenommen, in denen die empirische Forschung durchgeführt wurde und über die ggf. interne Informationen in den Dokumenten enthalten sind.

Nach Durchführung der notwendigen Maßnahmen zur Anonymisierung und Pseudonymisierung werden die Schadensrisiken noch einmal überprüft und die Freigabeklassen der Dokumente festgelegt.

Dritte Stufe: Vorbereitung zur Nachnutzung über Freigabeklassen in eLabour

Das FDZ eLabour stellt qualitative Forschungsdaten für die wissenschaftliche Nutzung zur Verfügung, nachdem sie im Rahmen einer datenschutzrechtlichen Prüfung mit einer eLabour-Freigabeklasse ausgezeichnet wurden. Mit dieser Freigabe werden Zugangsmöglichkeiten in Rahmen der eLabour Infrastruktur definiert und Auflagen festgelegt, die von NutzerInnen zu erfüllen sind.

Freigabeklassen in eLabour definieren abgestufte Zugangsmöglichkeiten zu den Forschungsdaten für wissenschaftliche Forschungszwecke. Voraussetzung ist ein Nutzungsvertrag mit dem FDZ eLabour, der die Nutzungsbedingungen für jede verwendete Studie im Einzelnen regelt. , die Weitergabe an Dritte ist untersagt.

Vor dem Zugang durch Nutzer werden die für die jeweilige Freigabeklasse definierten technischen und organisatorischen Maßnahmen durchgeführt, überprüft und dokumentiert. Erst danach kann der Zugang gewährt werden. Es wird ein Nutzungsvertrag geschlossen, der generell ein striktes Verbot der Re-Identifikation und der schriftlichen oder mündlichen Weitergabe persönlicher Merkmale der Studien-Teilnehmer oder sensibler Informationen über Personen umfasst. Durch den Nutzungsvertrag hat das FDZ eLabour die Kontrolle darüber, wer für welche Forschungszwecke das Material nutzt. Mit dem Nutzungsvertrag und der damit verbundenen kontrollierten Datennutzung wird das Restrisiko der nicht faktisch anonymisierten Forschungsdaten und deren unbefugte Verwendung abgefangen.

Die fünf Freigabeklassen definieren Zugangsmöglichkeiten, sowie die rechtlich und ethisch erforderlichen technischen und organisatorischen Schutzmaßnahmen und Auflagen zum Schutz von personenbezogenen Informationen in den qualitativen Daten.

Die erste Freigabeklasse beinhaltet keine weiteren Auflagen (neben der Zweckbindung für Wissenschaft und dem Verbot der Weitergabe), die fünfte Klasse verbietet den Zugang.

Die Freigabeklassen für empirische Dokumente sind wie folgt definiert (siehe ausführlicher in Anhang D):

FGK I: **Offener wissenschaftlicher Zugang** für registrierte WissenschaftlerInnen zum Lesen von qualitativen Daten ohne Schadensrisiko

FGK II: **Wissenschaftliche Nachnutzung** von qualitativen Daten mit geringem Schadensrisiko

FGK III: **Kontrollierte wissenschaftliche Nachnutzung** von qualitativen Daten mit mittlerem Schadensrisiko

FGK IV: **Beschränkte wissenschaftliche Nachnutzung** von qualitativen Daten mit hohem Schadensrisiko, externe Schadensfolgeabschätzung

FGK V: **Kein Zugang für qualitative Daten mit sehr hohem Schadensrisiko**

Für jede Freigabeklasse werden jeweils die notwendigen technischen und organisatorischen Maßnahmen festgelegt, die den Zugang und die Verwendung der geprüften und freigegebenen Forschungsdaten erlauben (siehe Anhang D). Sie werden in Nutzungsverträgen rechtsverbindlich vereinbart.

Der Zugang externer wissenschaftlicher NutzerInnen zu den Forschungsdaten wird durch eLabour gewährt und verantwortet. Gestützt auf die eLabour Infrastruktur wird dabei sichergestellt, dass die in der Risikoklassifikation und im Freigabeprozess festgelegten Zugangsmöglichkeiten und die technischen und organisatorischen Maßnahmen eingehalten werden.

4. Zusammenfassung und Grundprinzipien

Da Informationsgehalt und Anonymisierung in einem Spannungsverhältnis stehen, besteht die Herausforderung darin, einen Ausgleich zwischen Forschungs- und Datenschutzinteressen zu ermöglichen. Das Datenschutzkonzept von eLabour verfolgt das Ziel, dieses Spannungsfeld durch differenzierte Schadensfolgenabschätzung und daraus abgeleitete technische und organisatorische Datenschutzmaßnahmen aufzulösen, indem einerseits die Schutzrechte von untersuchten Personen und Organisationen gewahrt und gleichzeitig ein möglichst hohes Analysepotenzial der Forschungsdaten bewahrt wird. Dabei sollen möglichst wenige datenverändernde Maßnahmen stattfinden, sondern ein weitreichender Schutz der Befragten wird durch ergänzende organisatorische und technische Maßnahmen des Datenschutzes sichergestellt. **Es gilt die Maxime: So viel Informationen wie möglich für die Sekundäranalyse erhalten und so viel Informationen wie nötig durch Pseudonymisierung oder Anonymisierung schützen.**

Um diese Abwägung zu ermöglichen, wird eine **Risikoanalyse** der Datenbestände im Bedarfsfall bis hin zu den einzelnen Datensätzen durchgeführt. Als Ergebnis werden die Forschungsdatensätze in **Freigabeklassen** eingeteilt aus denen sich die erforderlichen **technischen und organisatorischen Maßnahmen** ergeben. Daten mit einem hohen personenbezogenen Risiko werden nur nach weitergehender **Datenschutzfolgeabschätzung** unter Einziehung externer GutachterInnen zugänglich gemacht.

Das Datenschutzkonzept gewährleistet so durch Regeln, Verfahrensweisen, technische wie organisatorische Maßnahmen einen Ausgleich zwischen den Interessen von Wissenschaft und Gesellschaft an der Nutzung von öffentlich finanzierten Forschungsdaten einerseits und den Anforderungen des Datenschutzes bzw. der teilnehmenden Personen andererseits in Bezug auf konkrete Forschungsdaten. **Andere Zwecke als die wissenschaftliche Nachnutzung sind ausgeschlossen.**

Anhänge

Die folgenden Anhänge sind derzeit aus Gründen der IT-Sicherheit in der öffentlichen Fassung nicht oder nicht vollständig enthalten:

Anhang A. Verfahrensdokumentation

Anhang B. Technische und organisatorische Maßnahmen (hier nur Einleitung)

Anhang B.
Technische und organisatorische Maßnahmen

Einleitung

Die Verarbeitung von personenbezogenen Forschungsdaten im Rahmen von eLabour dient unterschiedlichen, in Datenschutzkonzept und im Verfahrensverzeichnis (oben) näher beschriebenen Zwecken, hier verkürzt mit 1. Ingest der Forschungsdaten vom Datenhalter 2. Kuratierung und 3. Nachnutzung bezeichnet.

Im Rahmen des Ingest der Originaldaten verarbeitet eLabour die Daten im Auftrag mit dem Ziel der Langzeitarchivierung.

Die originalen Forschungsdaten werden im Rahmen der Kuratierung durch eLabour **im Auftrag** und in enger Kooperation mit dem Datenhalter bearbeitet. Gestützt auf IT-Tools werden sie **anonymisiert** oder **pseudonomysiert** und mit **Metadaten** versehen. Dieser Bearbeitungsschritt erfordert i.d.R. den **Zugriff auf eine Kopie der originalen Forschungsdaten**. Dieser Zugriff wird durch **Vertraulichkeitserklärungen** mit den individuellen WissenschaftlerInnenn geregelt. Die Verarbeitung dieser Daten erfolgt in einem privaten/abgeschirmten Bereich der VFU (privater Bereich). Dabei können auch die im Rahmen der Bearbeitung der Forschungsdaten erzeugten Metadaten in Bezug schutzwürdige Informationen enthalten. Dies betrifft insbesondere die Bezeichnungen von untersuchten Organisationen (typischerweise z.B. Firmennamen). Im Rahmen der VFU werden diese Daten durch geeignete organisatorische (**Nutzungsverträge**) und technische Maßnahmen (**sensible Metadaten werden abgestimmt nach Nutzerrollen aus- oder eingeblendet**) geschützt. Im Rahmen der **Anonymisierung** werden auf dieser Grundlage die notwendigen Maßnahmen durchgeführt und **dokumentiert**.

Die Verarbeitung durch die Mitarbeitenden von eLabour sowie der Zugriff durch Dritte im Rahmen der Nachnutzung erfolgt im Rahmen des Rollen- und Rechtekonzept, sowie des Freigabekonzepts, die beide im Weiteren ausführlich beschrieben sind. Im **Freigabeprozess** wird festgelegt, welche **Nutzergruppen** mit welchen Auflagen Zugang zu den Daten erhalten können. Diese Festlegungen werden IT-basiert umgesetzt und die Zugriffe **dokumentiert**. Der Freigabeprozess beinhaltet darüber hinaus die Basis für die Risikobewertung.

Die Verarbeitung erfolgt – physikalisch – auf der Hardware eines Auftragnehmers, der durch eine Vereinbarung zur Auftragsverarbeitung zur Einhaltung datenschutzrechtlicher Anforderungen verpflichtet ist. Die diesbezüglichen technischen und organisatorischen Maßnahmen werden durch den Auftragsverarbeiter (unten kurz: AV) abgebildet und ergeben sich aus der Dokumentation derselben in der Anlage 1 zu vorgenannter Vereinbarung.

Die nachfolgend dargestellten technischen und organisatorischen Maßnahmen sichern die Einhaltung datenschutzrechtlicher Vorgaben insbesondere im Sinne von Art. 32 DSGVO ab, soweit sie nicht bereits abschließend durch den Auftragsverarbeiter abgedeckt sind.

Die technischen und organisatorischen Maßnahmen können aus Sicherheitsgründen nicht veröffentlicht werden.

Anhang C. Rollen- und Rechtekonzept

Rollen beziehen sich immer auf bestimmte Studien, i.d.R. Primärstudien. Es können aber auch Sekundärstudien bzw. Sammlungen sein, die im Rahmen der Nachnutzung entstehen.

Die für die jeweilige Rolle festgelegten Rechte gelten grundsätzlich nur für Studien, für die die Rechte dem/der jeweilige/n RolleninhaberIn persönlich zugewiesen werden müssen. D.h. aber, **dass die Rollen i.d.R. für jede Studie im FDZ definiert werden können/müssen.**

Ausnahmen sind die Rollen StudyAdmin eines Instituts und **FreigabeAdmin** eines Instituts (diese sind verantwortlich für die Umsetzung und Kontrolle der Datenschutzmaßnahmen aller Studien des jeweiligen Instituts in Kooperation mit Datenschutzbeauftragter/m). Diese Rollen werden institutsbezogen besetzt, i.d.R. sollten immer zwei Personen pro Institut benannt sein. Institute oder WissenschaftlerInnen als DatenhalterInnen können auch MitarbeiterInnen aus eLabour beauftragen, insbesondere Admin's anderer Institute, wenn Sie nicht selbst diese Admin-Rollen besetzen können oder wollen.

Wir unterscheiden Rollen innerhalb von eLabour von externen User Rollen auf der Basis von Nutzungsverträgen. Interne Rollen regeln die Rechte im Ingest- (T1) und im Kurationsprozess (T2). Externe Rollen gewähren Zugangsrechte für die Nutzung in T3.

Der Begriff **Institut** wird synonym für ForschungspartnerInnen in und von eLabour verwendet. Dies sind die aktuellen VerbundpartnerInnen, zukünftig Forschungseinrichtungen unterschiedlicher Art, mit denen Kooperationsvereinbarungen getroffen werden, in denen die Art der Zusammenarbeit festgelegt ist.

Interne Rollen und Rechte

Institute und/oder DatenhalterInnen benennen mindestens einen Freigabe-Admin und einen Study-Admin. Es können auch mehrere Personen mit diesen Rollen betraut werden. Freigabe-Admin und Study-Admin sollen nicht die gleichen Personen sein, damit immer Vier-Augen in die Bewertung involviert sind.

Die Rolle des Freigabe Admin berechtigt zur Festlegung von Freigabeklassen und zur Freigabe von Dokumenten. Die Festlegung von Freigabeklassen ist zu protokollieren, Begründungen sind schriftlich festzuhalten, in einfachen Fällen kann dies standardisiert geschehen.

Die beiden Rollen auf Institutsebene – Study-Admin und Freigabe-Admin – stehen in einer engen Wechselbeziehung, durch die für wichtige (datenschutzrechtliche) Entscheidungen ein vier-Augen-Prinzip realisiert wird, i.d.R. macht der Study Admin Vorschläge, die der Zustimmung durch den Freigabe Admin bedürfen. Umgekehrt basieren Entscheidungen des Freigabe Admins auf Vorarbeiten und Vorschlägen des Study Admins (noch zu prüfen: Wie können bestimmte Änderungs-Aktivitäten mit dem Namen der Person dokumentiert werden?)

StudyAdmin

Die zentralen Aufgaben des StudyAdmin sind der Ingest der Forschungsdaten, die Verwaltung und Bearbeitung der Studien des jeweiligen Instituts in T1 und T2, sowie die Unterstützung des Freigabe-Admin in Freigabeprozess;

Study-Admin hat alle Bearbeitungsrechte bezogen auf die Forschungsdaten der Studien „seines" Instituts; mind. 2 Personen sollten pro Institut Study Adminrechte haben:

- Verwaltet Original-Studien des Instituts in T1 (im persönlichen Bereich des eLabour Portals)
- Verwaltet Studien des Instituts in T2 (dem Bereich in dem die Forschungsdaten aufbereitet, Datenschutzmaßnahmen durchgeführt und ergänzt werden)
- Import via Ingest-Tool (in T1 und T2)
- Anlegen, Organisieren, Ändern, Lesen von Dokumenten der Studien und der Metadaten via GUI
- Lädt Study EditorInnen ein, Einladung muss von Freigabe Admin des Instituts bestätigt werden
- Benannt von einem Institut oder Forschungseinheit (mit Kooperationsvertrag) und nach Einweisung durch dafür verantwortliche Personen aus eLabour

StudyEditor

Aufgabe ist die Bearbeitung bestimmter, zugewiesener Studien in T2, die Eingabe von Metadaten und die Ergänzung von Daten, sowie Erstellung von Dokumentationen für Archivierung und Kuration der Daten

- Eingeladen von einem Study Admin zur Bearbeitung bestimmter Studien **in T2**
- Verwalten via GUI, d.h. Ergänzen von Metadaten, Erstellen und Hochladen von Dokumenten in dieser Studie
- Bearbeiten von Dokumenten der Studie mit Anwendungssoftware
- Voraussetzung: Benennung durch Institut und Einweisung in GUI und Metadatenmodell durch dafür verantwortliche eLabour MitarbeiterIn

StudyRiskEditor

Aufgabe ist die Durchführung von Anoymisierung bzw. Pseudonymisierung und Risikobewertung von empirischen Dokumente von bestimmten, zugewiesenen Studien in T2; Dies umfasst das Anlegen neuer, bearbeiteter Versionen empirischer Dokumente, Änderung von Dokumenten, Erstellen von Dokumentationen, Vorschläge für Freigabeklassen und Metadateneingaben.

- Eingeladen von einem Study Admin für datenverändernde Datenschutzmaßnahmen, Dokumentation und Ergänzung der Metadaten für zugewiesene Studien
- Durchführung von Anonymisierung, Pseudonymisierung, Risikoanalyse, Freigabeklassen im Rahmen des festgelegten Workflows mit Anwendungssoftware
- Eingabe und Änderung von Metadaten und Dokumenten in GUI
- Voraussetzung: durch Einweisung und Training nachgewiesene Kompetenzen für Datenschutz, Risikoanalyse und jew. Anwendungssoftware + GUI

FreigabeAdmin

- Prüfung und Entscheidung über die vorgeschlagenen Freigabeklassen für die Dokumente der Studien des Instituts
- Freigabe auf Studien- und Dokumentenebene
- Prüfung der jeweiligen freigabeklassenspezifischen Voraussetzungen, Festlegung der Zugangsbedingungen und Vorbereitung der Nutzungsverträge für vom Nutzer beantragte Studie des Instituts (aufgrund von Standardverträgen)

WissStudyOwner

Rolle für WissenschafltlerInnen als PrimärforscherInnen und Datenhalter

Die Rolle des wissenschaftlichen Study Owners ist für Primärforschende und Wissenschaftler

vorgesehen, die entweder eigenständig die von ihnen maßgeblich (mit-)erzeugten Forschungsdaten im FDZ ablegen, dort bearbeiten oder die Ihre eigenen Daten ohne Freigabe für Dritte für eigene Sekundärforschung nutzen wollen. Diese Rolle ist vorgesehen, sollte aber nicht standardmäßig für jede Studie und für alle Primärforschenden vergeben werden, sondern nur auf Anfrage und möglichst begrenzt auf bestimmte Verarbeitungsmöglichkeiten und Daten. Sie wird insbesondere für solche Studien benötigt, die in den ersten 10-20 Jahren aufgrund besonders sensibler Daten nicht für die externe Nutzung freigegeben werden sollen.

- Verwaltet eigene Studiendaten in T1 (im persönlichen Bereich des eLabour Portals)
- Anlegen, Organisieren, Ändern der eigenen Studie
- Hat Lese und Download-Zugriff auf eigene Studie/n via FDM Portal und Suche
- Hat Zugriff auf GUI zum Ergänzen von Metadaten und Hochladen von Dokumenten
- Kann eigene Sekundärstudien (Sammlungen) anlegen, bearbeiten und verwalten
- Die Freigabe für weitere User bedarf einer Entscheidung der Freigabe Admins eines Instituts

Externe Nutzer-Rollen und Rechte

NutzerInnen erhalten Zugriff auf die für sie freigegebene Studie in T3, für die ein Nutzungsvertrag besteht.

Die Zugriffsrechte sind abhängig und definiert durch die jeweilige Freigabeklasse auf den Ebenen Studie, Fall und Dokumente, sowie durch den Nutzungsvertrag, der die Rechte und Pflichten konkretisiert und vertraglich festlegt.

Nutzer1 mit Registrierung als WissenschaftlerIn und einfachem Nutzungsvertrag zum Lesen mit Remote Zugang (FGK I)

- Zugang zu allgemeinen Studieninformationen für alle freigegebenen Studien im FDZ eLabour
- Zugang zu registrierter Studie FGK I mit Remote-Access zum Lesen

Nutzer2 mit Nutzungsvertrag für Studie mit Remote-Access und Downloadmöglichkeit (FGK II und FGK III)

- Zugang zu allgemeinen Studieninformationen für alle freigegebenen Studien im FDZ eLabour
- Zugang zu den Dokumenten der für den Nutzer freigegebenen Studie, die nicht in FGK IV oder V sind
- Auflagen und Beschränkungen wie vereinbart

Nutzer3 mit Nutzungsvertrag für Studie mit Remote-Access ohne Downloadmöglichkeit (FGK IV)

- Zugang zu allgemeinen Studieninformationen für alle freigegebenen Studien im FDZ eLabour
- Zugang zu den Dokumenten der für den Nutzer freigegebenen Studie mit FGK IV
- Auflagen und Beschränkungen wie vereinbart

Anhang D. Risikobewertung, Freigabeklassen und Zugangsmöglichkeiten für qualitative, soziologische Forschungsdaten im FDZ eLabour

Das FDZ eLabour stellt qualitative, soziologische Forschungsdaten für die wissenschaftliche Nachnutzung zur Verfügung, nachdem sie im Rahmen einer datenschutzrechtlichen Prüfung mit einer eLabour-Freigabeklasse ausgezeichnet wurden. Mit dieser Freigabe werden Zugangsmöglichkeiten in Rahmen der eLabour Infrastruktur definiert und Auflagen festgelegt, die von Nutzern zu erfüllen sind.

Im Folgenden werden die eLabour-Freigabeklassen und der Prozess der datenschutzrechtlichen Prüfung (Schadensrisikobewertung der Forschungsdaten) festgelegt. Es werden Benutzerrollen und Rechte innerhalb von eLabour beschrieben, die im Prozess der Prüfung und Freigabe benötigt werden; Sowie Rollen und Rechte von externen Nutzern des FDZ eLabour.

Überblick

Vor der Freigabe werden die im FDZ eLabour aufgenommen qualitativen Forschungsdaten im Zuge der Bearbeitung, Kuratierung und Archivierung einer manuellen Risikobewertung unterzogen, aus der notwendige Datenschutzmaßnahmen und Zugangsmöglichkeiten abgeleitet werden.

Die Freigabeklassen in eLabour ermöglichen abgestufte Zugangsmöglichkeiten zu den Forschungsdaten für WissenschaftlerInnen[1] für die wissenschaftliche Nutzung. Hierfür schließen sie einen Nutzungsvertag mit dem FDZ eLabour ab, der die Nutzungsbedingungen für jede der verwendeten Studien im Einzelnen regelt, Re-Identifikation sowie schriftliche oder mündliche Weitergabe personenbezogener Informationen an Dritte ist untersagt (Ausnahmen durch Anwendung von Archivrecht für Studien vor 1980 können im Einzelfall geprüft werden).

Die fünf Freigabeklassen definieren auf einer aufsteigenden Skala die rechtlich und ethisch notwendigen Einschränkungen und Auflagen zum Schutz potentiell noch personenbezogener, qualitativer Daten (s.u.).

Risikobewertung, Pseudonymisierung und Vergabe von Risikoklassen

Die Risikoklassen werden in einem Prozess definiert, bei dem jedes Dokument, das freigegeben werden soll, einer manuellen Prüfung (Lesen des Dokuments) unterzogen wird.

Die Intensität der manuellen Prüfung ergibt sich aus der Risikoeinschätzung auf der Ebene der Studie und des Falls.

In der ersten Stufe werden die Dokumente gelesen, Klarnamen der TeilnehmerInnen werden entfernt und pseudonymisiert und sensible, personenbezogene Informationen werden markiert oder pseudonymisiert und bearbeitet (siehe Verfahren der Risikobewertung). Ergebnis dieser Stufe sind formell anonymisierte Datensätze, ein standardisiertes Risikobewertungsprotokoll und ggf. ein Auszug sensibler Textstellen. In jedem Fall wir auf der Fallebene eine dokumentierte Schlüsseltabelle zur

[1] WissenschaftlerInnen sind Mitarbeiter von öffentlichen Forschungseinrichtungen oder Universitäten bzw. öffentlich geförderten Forschungsprojekten; über Anträge von anderen WissenschaftlerInnen muss im Einzelfall von der GF entschieden werden. Kriterium sind öffentlich geförderte Forschungszwecke.

Dokumentation erzeugt, bei den neueren Studien (digital erzeugt) zusätzlich eine Dokumentation für jedes Dokument.

Risikomerkmale (kann ergänzt werden)

- Grad und Art des Schadensrisikos für die Person
- besonders schutzwürdige personenbezogene Daten
- Erhebungszeitraum
- Re-Identifikationsrisiko der Person
- Schadensrisiken für die Organisation

Wesentlich für die Einschätzung über das in den Dokumenten enthaltene Risiko für befragte Personen und Unternehmen ist, neben den erhobenen Daten, das Alter der Studie und die Einschätzung von Seiten der PrimärforscherInnen. Daher werden die PrimärforscherInnen, bevor die Arbeit an den Dokumenten beginnt, zu ihrer Einschätzung bzgl. der Brisanz der erhobenen Daten aus heutiger Perspektive, sowie über getroffene Absprachen mit den Unternehmen und Personen befragt. Danach beginnt die Arbeit am Dokument, welches das genaue Lesen dieser impliziert, um zu einer Risikoeinschätzung zu gelangen.

Für die Dokumentation der Risikoanalyse kommen zwei Tabellen (siehe Anlage) zum Einsatz. In der Risikotabelle werden alle Daten erfasst, welche für die Risikoeinschätzung relevant sein können. Hierzu zählen neben Klarnamen der Befragten kritische Informationen über das Unternehmen, sowie persönliche Angaben über den/die Befragte/-n. Textpassagen, die kritische Informationen enthalten, werden im Text markiert, sodass sie automatisch extrahiert werden können. Auf die so erzeugten Daten kann bei der Vergabe der Freigabeklassen zurückgegriffen werden. Die Klarnamen der befragten Personen werden pseudonymisiert und in eine Schlüsseltabelle eingetragen. Die Schlüsseltabelle wird separat abgelegt und dient dazu erstens sicherzustellen, dass keine Pseudonyme doppelt vergeben werden und zweitens stellt sie die Verbindung der bearbeiteten Datei und der Originaldatei sicher. Dies ist notwendig, da die Dateien beim Ingest neue, automatisch generierte Bezeichnungen zugewiesen bekommen. Identifizierende Informationen die das Unternehmen betreffen werden nicht aus den Dokumenten entfernt. Dies hat den Hintergrund, dass ein Großteil der Dokumente für die Sekundäranalyse so unbrauchbar gemacht würden. Über den abgeschlossenen Nutzungsvertrag wird jedoch sichergestellt, dass die Anonymität der Unternehmen gewahrt bleibt. Nachdem die Dokumente so bearbeitet wurden treffen die BearbeiterInnen eine Einschätzung bzgl. des vorhandenen Risikos für die befragten Personen und Unternehmen. Auf diese Einschätzung wird sich bei der Vergabe der Freigabeklasse bezogen. Vor der Veröffentlichung in T3 werden die Markierung entfernt, lediglich die anstelle der Klarnamen vergebenen Pseudonyme bleiben in den Texten enthalten.

Einen Sonderfall stellen Studien dar, welche auf Grund ihres Alters und der erhobenen Daten (Einschätzung der PrimärforscherInnen), besonders risikoarm sind. In diesem Fall kommt eine reduzierte Risikotabelle zum Einsatz, in der lediglich die vergebenen Pseudonyme und kritische Passagen (mit Seitenangabe), sowie die Risikoeinschätzung festgehalten werden. Bei diesen Dokumenten handelt es sich um OCR erkannte Dateien (pdf Format), die nicht mit dem oben beschriebenen Verfahren markiert werden können. Klarnamen werden geschwärzt und das Dokument erneut gespeichert, sodass die Schwärzung nicht rückgängig gemacht werden kann.

Auf Grundlage dieser Risikoanalyse wird der Freigabeprozess vom FreigabeAdmin durchgeführt.

Freigabeklassen für die Weitergabe der qualitativen Daten an Dritte

Die Festlegung der Freigabeklasse (durch den FreigabeAdmin) basiert auf der Risikoklassifikation,

ergibt sich aber nicht automatisch hieraus. Sie erfolgt fallweise für jedes Dokument des Falls bzw. der Studie.

Im Freigabeprozess werden die im Rahmen der Risikoanalyse dokumentierten, personenbezogenen Informationen im Zusammenhang bewertet, ggf. kann die Risikoklasse auf dieser Grundlage korrigiert oder in einzelne Dokumenten zusätzliche Pseudonymisierungen vorgenommen werden.

Für jede Freigabeklasse sind jeweils die technischen und organisatorischen Maßnahmen definiert, die den Zugang und die Verwendung der geprüften und freigegebenen Forschungsdaten erlauben (siehe Abschnitt B). Sie werden in Nutzungsverträgen rechtsverbindlich vereinbart.

Mit der Freigabeklasse werden die Zugangsmöglichkeiten (Nachnutzung mit Remote-Access-Zugang und ggf. Download der Daten), sowie Nutzungseinschränkungen und Kontrollmöglichkeiten für das FDZ eLabour definiert. Schließlich spielt auch die Person des Nutzers (z.B. Insiderwissen) und der Zweck der wissenschaftlichen Nutzung eine Rolle. Die erste Freigabeklasse beinhaltet keine weiteren Auflagen (neben der Zweckbindung für Wissenschaft und dem Verbot der Re-Identifikation und der Weitergabe), die fünfte Klasse verbietet einen Zugang für die wissenschaftliche Nachnutzung.

Tabelle D1 Freigabeklassen

Freigabe-klasse	Risikoklasse	Benennung, Zugangsmöglichkeiten und Nutzungsbedingungen
FGK I	Daten ohne Schadensrisiko	**Offener wissenschaftlicher Zugang** für registrierte WissenschaftlerInnen; Zugang Remote-Access nur zum Lesen von Studienbeschreibungen und Daten ohne Schadensrisiko
FGK II	Daten mit geringem Schadensrisiko	**Wissenschaftliche Nutzung** von qualitativen Daten mit geringem personenbezogenen Schadensrisiko; Zugang Remote-Access und Downloadmöglichkeit
FGK III	Daten mit mittlerem Schadensrisiko	**Kontrollierte wissenschaftliche Nutzung** von qualitativen Daten mit mittlerem personenbezogenem Schadensrisiko; Zugang Remote-Access und Downloadmöglichkeit, Nachweis notwendiger Datenschutzmaßnahmen beim Nutzer, Vorlage von Zitaten mit Personenbezug vor Veröffentlichung[2], Ausschluss von Insidern
FGK IV	Daten mit hohem Schadensrisiko	**Eingeschränkte wissenschaftliche Nutzung** von qualitativen Daten mit hohem Schadensrisiko; Remote-Access Zugang, Nachweis notwendiger Datenschutzmaßnahmen beim Nutzer, Kontrolle von Ergebnissen vor der Veröffentlichung[3], Ausschluss von Insidern; externe Schadensfolgeprüfung
FGK IV	Daten mit sehr hohem Schadensrisiko	**Keine Zugangsmöglichkeit für Dritte**

In die Entscheidung über die Freigabeklasse geht immer eine Abwägung zwischen dem berechtigten Schutzbedürfnis der untersuchten Personen und Organisationen einerseits und dem öffentlichen Interesse an der wissenschaftlichen Forschung und Nachnutzung der i.d.R. mit öffentlichen Mitteln

[2] Vorlage von Ergebnissen bezieht sich nur auf Ergebnisse, die Informationen mit Personenbezug aus Dokumenten der FGK III enthalten.
[3] Kontrolle von Ergebnissen bezieht sich nur auf Ergebnisse, die Informationen mit Personenbezug aus Dokumenten der FGK IV enthalten.

erzeugten Daten andererseits ein. Da das Schadensrisiko oft innerhalb einer Studie, eines Falls und zwischen den Erhebungsarten unterschiedlich ist, ermöglicht der im FDZ eLabour auf der Dokumentenebene durchgeführte Risikobewertungs- und Freigabeprozess eine angemessene, differenzierte Abwägung zwischen Datenschutz und wissenschaftlichem Interesse.

Freigabeklassen können auf Ebenen Studie, Fall/Welle, Art der Erhebungsmaßnahme und Dokument vergeben werden. Sie müssen aber nicht auf jeder Ebene vergeben werden. Ist keine Freigabeklasse vergeben, ist kein Zugang zu den Informationen und Dokumenten der jeweiligen Ebene möglich. Dies betrifft auch die generellen Informationen zu einer Studie, sie sollten auf Qualität und Datenschutzanforderungen geprüft werden, bevor die Studie sichtbar ist. Das gleiche gilt auch für die Ebenen darunter (Fälle, Publikationen, Kontextmaterial).

Insbesondere bedeutet dies, dass kein empirisches Dokument ohne eine explizite (manuelle) Freigabeentscheidung bezogen auf dieses Dokument freigegeben werden kann (Änderung: „Vererbung“ von Freigaben von einer höheren Ebene ist aus rechtlichen und ethischen Gründen nicht vorgesehen).

Allerdings sollen die Freigaben und deren Begründung von den höheren Ebenen bei der manuellen Risikobewertung und Freigabe auf den darunter liegenden Ebenen berücksichtigt werden. Dabei gilt, dass höhere Freigabeklassen (sensiblere Daten) auf einer tieferen Ebene nur mit Begründung unterschritten werden dürfen.

Freigabeklassen auf der Ebene von Studie oder Fall oder Typ der Erhebungsmaßnahme (Dokumententyp in der Ordnerstruktur) berücksichtigen gemeinsame Merkmale, solche sind z.B. wie lange die Erhebung zurückliegt; ob die wissenschaftliche Fragestellung (Studienebene) systematisch besonders schutzwürdige Daten und/oder leicht zur Re-Identifikation der TeilnehmerInnen führende Daten generiert. Oder ob es Einverständniserklärungen, Absprachen, Zusicherungen gegenüber Organisationen, Unternehmen, Gruppen (Fallebene) gibt, die weiter gehende Freigaben nicht zulassen (solange die Daten nicht vollständig anonymisiert sind). Oder es gibt Vorgaben für bestimmte Erhebungsmaßnahmen (z.B. Expertengespräche), die auf Einschätzungen der PrimärforscherInnen und/oder Vorerfahrungen beruhen.

Diese Voraussetzungen werden möglichst beim Anlegen der Studie oder des Falls /der Welle oder des Typs der Erhebungsmaßnahme geprüft und geeignete Freigabeklassen für die jeweilige Ebene vergeben. Sinnvoll scheint eine automatisierte (IT-gestützte) Kontrolle der Freigabeklassen von Dokumenten bei deren Vergabe, ob diese von den Freigabeklassen höherer Ebenen oder den Risikoklassen (siehe Tabelle 1) abweichen. Für diesen Fall kann eine Warnung erfolgen und eine Begründung eingefordert werden (z.B. Nennung eines zulässigen Grundes, die in geeigneter Weise dokumentiert wird).

Freigaben auf der Ebene von Dokumenten setzen den Nachweis voraus, dass eine Risikoanalyse durchgeführt wurde und dass deren Ergebnis im Rahmen der o.g. Tabelle zu der gewählten Freigabeklasse passt. So wird sichergestellt, dass durch auf der Ebene von Studien oder Fall vergebene Freigabeklassen zur Freigabe von Dokumenten führen, die keiner Risikoanalyse unterzogen wurden oder deren Ergebnis nicht mit o.g. Tabelle übereinstimmt. Freigaben auf der Ebene der Dokumente müssen die Freigabeklassen der höheren Ebene berücksichtigen. Wird eine abweichende, niedrigere Freigabeklasse für Dokumente gewählt, so muss dies im Protokoll der Freigabe begründet werden, z.B. mit durchgeführten datenverändernden Maßnahmen (Pseudonymisierung / Anonymisierung), Ablauf von Sperrfristen, etc.

Ist (noch) keine Freigabeklasse definiert oder wird die Freigabeklasse 5 aktiv vergeben, so ist keine Freigabe möglich. Solche Dokumente sind nicht für die Nutzung zugänglich, sondern dürfen lediglich von den Datenhaltern zum Zweck der gemeinsamen Bearbeitung im Rahmen von eLabour dafür

berechtigten Personen zugänglich gemacht werden.

Freigabe und Nutzungsverträge

Da die qualitativen Forschungsdaten in eLabour mit möglichst wenigen datenverändernden Maßnahmen verfügbar gemacht werden, wird der Zugang durch Nutzungsverträge geregelt, die weitreichende Transparenz und Kontrolle der Nachnutzung ermöglichen. Durch den Nutzungsvertrag hat das FDZ eLabour die Kontrolle darüber, wer für welche Forschungszwecke das Material nutzt. Mit dem Nutzungsvertrag und der damit verbundenen kontrollierten Datennutzung wird das Restrisiko der nicht faktisch anonymisierten Forschungsdaten und deren unbefugter Verwendung abgefangen.

Alle Nutzungsverträge beinhalten ein Verbot der Re-Identifikation von Personen und Organisationen, es sei denn, Personen oder Organisationen sind bereits durch Veröffentlichungen, z.B. der Primärforschenden bekannt. Weiterhin beinhalten sie ein Verbot der schriftlichen und/oder mündlichen Weitergabe ggf. noch in den qualitativen Daten enthaltener nicht anonymisierter, personenbezogener Informationen, sowie ggf. die Verpflichtung Informationen über Organisationen vertraulich zu behandeln, sofern die Primärforschenden eine solche Vertraulichkeit zugesichert haben.