Medizinische Soziologie, Institut für Epidemiologie und Präventivmedizin, Universität Regensburg

Datensicherheits- und Datenschutzkonzept

Version 1.0 vom 01.05.2021

Inhalt

1. Einleitung

Das vorliegende Konzept beschreibt Maßnahmen zur Datensicherheit und Datenschutz der Medizinischen Soziologie des Instituts für Epidemiologie und Präventivmedizin der Universität Regensburg.

Beratung durch den Datenschutzbeauftragten

Das Datenschutzkonzept wurde unter Mitwirkung des Datenschutzbüros der Universität Regensburg erstellt.

Informationen zum Server

Die Daten der Medizinischen Soziologie werden auf dem Titan-Server des Rechenzentrums der Universität Regensburg gespeichert und können nur von befugten Personen (= Mitarbeiter/innen, Doktorand(inn)en, Hilfskräfte, die aktiv in ein entsprechendes Projekt einbezogen sind) verarbeitet werden.

Die Zugriffssteuerung erfolgt über das Berechtigungssystem der zugrundeliegenden File-Server der Firma Microfocus. Die Verfügbarkeit der Daten wird einerseits durch den Cluster-Betrieb der File-Server und andererseits durch das Backup-Konzept des Rechenzentrums gewährleistet.

2. Einwilligung, Widerruf

Alle möglichen Studienteilnehmer/innen erhalten vor Beginn der Teilnahme an einem Forschungsprojekt in mündlicher und schriftlicher Form eine detaillierte Aufklärung über Zweck und Inhalte der Studie. Sie werden über den genauen Ablauf der Studie sowie über mögliche Risiken, die mit der Teilnahme an der Studie verbunden sind, aufgeklärt. Alle Teilnehmer/innen unterschreiben vor Beginn der Teilnahme eine Einverständniserklärung hinsichtlich Umgang und Weiterverarbeitung der personenbezogenen und neu generierten Daten. Sie werden in mündlicher und schriftlicher Form darüber informiert, dass die Teilnahme zu jedem Zeitpunkt ohne Angabe von Gründen in mündlicher oder schriftlicher Form widerrufen werden kann. Der dazugehörige Datensatz wird dann anonymisiert und personenbezogene Daten gelöscht. Teilnehmer/innen werden außerdem darüber aufgeklärt, dass ihnen durch den Widerruf kein Nachteil entsteht.

3. Zutritts, Zugriffs- und Zugangskontrolle der Daten

Zutrittskontrolle

Die Räume und Büros der Medizinischen Soziologie sind nur für die Mitarbeiter/innen mittels entsprechender Schlüssel zugänglich. Die Schlüssel werden gegen eine persönliche Unterschrift ausgehändigt und nach Ausscheiden aus dem Team der Medizinischen Soziologie wieder abgegeben. Doktorand/innen und Hilfskräfte haben keinen eigenen Schlüssel zu den Büroräumen der Medizinischen Soziologie und arbeiten nur in den Räumlichkeiten, wenn ein/e Mitarbeiter/in anwesend ist. Längerfristig beschäftigte Doktorand/innen oder Hilfskräfte können in Rücksprache mit dem Team einen Schlüssel erhalten, sollte dies für deren Arbeit unerlässlich sein.

Zugangskontrolle

Alle lokalen und mobilen Rechner der Medizinischen Soziologie sind jeweils mit persönlichem Passwort sowie Bildschirmschoner (15 Minuten Zeitspanne) mit Passworteingabe bei Reaktivierung eingerichtet. Eine manuelle Aktivierung der Bildschirmsperre durch die Nutzer/innen muss ebenfalls möglich sein. Bei Verlassen des Arbeitsplatzes ist die Bildschirmsperre durch die Mitarbeiter/innen zu aktivieren. Einem potenziellen Zugang zu Daten durch Dritte bei kurzer Abwesenheit einer/s Mitarbeiter/in wird so entgegengewirkt. Passwörter werden alle 90 Tage erneuert. Schriftlich vorhandene Daten werden in abschließbaren Schränken aufbewahrt.

Zugriffskontrolle

Die Medizinische Soziologie arbeitet mit einem Rechnernetz mit individuell definierten Zugangsberechtigungen für jede/n Mitarbeiter/in, die von der Leitung der Medizinischen Soziologie festgelegt und von den für die IT zuständigen Mitarbeiter/innen entsprechend eingerichtet werden.

Die Datenbestände sind auf dem Server der Medizinischen Soziologie in projektbezogenen Ordnern sortiert. Zugriff zu diesen Ordnern erhalten jeweils nur befugten Personen. Ausgenommen sind Personen, welche nicht in dieses Datenschutzkonzept eingewilligt haben. Die Authentifizierung befugter Personen erfolgt via Benutzername und Passwort.

Im Rahmen der Benutzerkontrolle (Zugangsschlüssel, Mitarbeiterpasswort, Definition von Arbeitsgruppen) ist gewährleistet, dass auf projektbezogene Daten, einschließlich schutzwürdiger persönlicher Daten oder Sozialdaten, nur befugte Personen zugreifen können. User accounts werden umgehend nach Ausscheiden eines/r Mitarbeiter/in bzw. Beendigung eines Dissertationsverfahrens deaktiviert und die Zuordnung zum Projekt gelöscht.

Für schutzwürdige papiergebundene Daten und Sicherungskopien auf externen Datenträgern stehen Schränke mit hoher Brandschutzklasse im Keller der Medizinischen Soziologie zur Verfügung. Zugang zu diesen Schränken hat nur die Leitung der Medizinischen Soziologie.

4. Datenträgerkontrolle

Personenbezogene Daten oder pseudonymisierte Daten werden ausschließlich innerhalb der Medizinischen Soziologie unter den beschriebenen Zugangsbeschränkungen gespeichert und verarbeitet. Die Daten befinden sich auf einem Server der Universität Regensburg bzw. auf einen speziell dafür eingerichteten Rechner ohne Verbindung zum Netz (netzunabhängiger Rechner). Eine Speicherung von personenbezogenen Daten auf mobilen Datenträgern (USB-Sticks, CD/DVD oder Magnetbändern von Backups) soll vermieden werden und ist grundsätzlich nur zulässig, wenn die Dateien nach dem aktuellen Stand der Technik verschlüsselt sind und das Passwort geheim gehalten wird.

Müssen bei einzelnen Projekten sehr große Datenmengen verarbeitet werden, die die Kapazität des Servers übersteigen, erfolgt nach projektbezogener Begründung und Dokumentation keine Speicherung und Sicherung auf dem Server, sondern auf zugangsbeschränkten lokalen Rechnern namentlich für die einzelnen Projekte sowie auf externen Festplatten. In diesen Fällen werden alle Dateien mittels Passwort gegen den Zugriff Dritter geschützt.

Externe Festplatten werden verschlossen aufbewahrt und entsprechend passwortgeschützt, um sie

vor dem Zugriff Unbefugter zu schützen. Die Verwendung von mobilen Rechnern für Zwecke der Datensicherung, institutseigene oder private Rechner, ist ausgeschlossen.

Neben dem persönlichen Zugang werden alle Speicherstandorte von Daten innerhalb des Netzwerks dokumentiert und auf Übereinstimmung mit den Zugangsregelungen überprüft.

Alle Passwörter zur Sicherung externer Datenträger, Transkripte und anderer Datenquellen werden auf einem passwortgeschützten Computer ohne Internetzugang in den Räumlichkeiten der Medizinischen Soziologie gesammelt. Sodass auch nach Ende der Projektarbeit der Zugriff auf erhobene Daten gewährleistet ist. Der Zugang zu diesem Computer ist nur wenigen ausgewählten Personen (Projektleiter(innen), Projektkoordinator(innen)) gewährt.

Die Gestaltung und der Gebrauch von Passwörtern orientiert sich nach den Empfehlungen des Bundesamt für Sicherheit in der Informationstechnik (https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html).Passwörter sollten somit aus Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen bestehen. Es sollten mindestens zwei dieser Zeichenarten verwendet werden. Die Länge des Passworts sollte mindestens 8 Zeichen sein. Passwörter werden spätestens alle 90 Tage gewechselt. Zur Speicherung der Passwörter können Passwort-Speicher-Tools genutzt werden.

5. Weitergabekontrolle

Quantitative Studien

Die bei quantitativen Studien eingesetzten Fragebögen werden ausschließlich direkt an die Medizinische Soziologie zurückgeschickt, dort von autorisierten Personen geöffnet und in eine Datenbank eingegeben. Es erfolgt keinerlei Weitergabe.

Qualitative Studien

Audiodateien können elektronisch an eine studentische Hilfskraft oder ein Transkriptionsbüro übermittelt werden. Die Übermittlung der Daten findet elektronisch über eine gesicherte Internetverbindung oder über ein gesichertes externes Speichermedium (z.B. USB Stick) statt. Das Transkriptionsbüro sichert über eine Vertraulichkeitserklärung zu, dass sämtliche Daten auch über die Projektlaufzeit hinaus vertraulich behandelt werden und eine vollständige Löschung der Daten nach Abschluss des Projektes erfolgt. Die Rücksendung der transkribierten Dateien erfolgt ebenfalls über eine gesicherte Internetverbindung oder passwortgeschützt. Den Beteiligten werden die Anweisungen zum sicheren Löschen ausgehändigt, so dass die Dateien nach der Ver- oder Bearbeitung sicher gelöscht werden können.

Auch an institutsinterne Arbeitsgruppen werden Transkripte nur anonymisiert elektronisch verschickt. Den Beteiligten werden die Anweisungen zum sicheren Löschen ausgehändigt, so dass die Dateien nach der Ver- oder Bearbeitung sicher gelöscht werden können.

6. Kontrolle der Dateneingabe

Die Löschung von personenbezogenen Daten oder pseudonymisierten Daten nach Ablauf der Forschungsprojekte und in wissenschaftlichen Standards festgelegten Fristen wird protokolliert. Die Löschung personenbezogener Daten erfolgt nach Ablauf der Zwecke, für die die Daten erhoben wurden, spätestens nach Ablauf des Forschungsvorhabens. Die Löschung erfolgt durch technische Mittel, so

dass Daten von niemandem mehr zur Kenntnis genommen werden können. Details können in den jeweiligen projektspezifischen Datenschutzkonzepten bestimmt werden.

Quantitative Daten

Dokumente mit personenidentifizierbaren Daten (Einwilligungserklärungen) werden von befugten Personen entgegengenommen. Die darauf enthaltenen Informationen werden von diesen Personen auf einen netzunabhängigen Rechner übertragen. Der Rechner ist passwortgeschützt und nur für befugte Personen zugänglich. Nach Übertragung der Angaben werden die Dokumente getrennt von den Studiendaten in verschlossenen Schränken gelagert. Studiendokumente (pseudonymisierte Fragebögen) werden ebenso durch befugte Personen bearbeitet. Nach der Übertragung werden die Studiendaten in den Räumen der Medizinischen Soziologie in verschlossenen Schränken gelagert.

Qualitative Daten

Die Transkription der Audiodateien erfolgt durch befugte Personen oder externe Transkriptionsbüros. Die Anonymisierung erfolgt direkt während der Transkription oder wird in einem gesonderten Schritt nach der Transkription (z.B. nach Transkription durch ein Transkriptionsbüro) durchgeführt.

Nach Überspielung der Audiodatei auf einen gesicherten Rechner werden die Daten unverzüglich auf dem Aufnahmegerät gelöscht. Nach Fertigstellung des anonymisierten Transkripts werden die Audiodateien in einem dafür vorgesehenen netzunabhängigen Rechner 10 Jahre aufbewahrt. Zugang zu diesem Rechner haben nur befugte Personen der Medizinischen Soziologie. Dieser Rechner ist ebenfalls passwortgesichert.

Nicht-anonymisierte Transkripte werden passwortgesichert und nicht ausgedruckt. Bei computerbasierter Auswertung (z.B. mit Atlas.ti) werden nur anonymisierte Transkripte in das Programm eingelesen.

7. Anonymisierung bzw. Pseudonymisierung bei der Datenverarbeitung

Quantitative Studien

Das Vorgehen bei der Pseudonymisierung baut auf den von der Technologie- und Methodenplattform für vernetzte medizinische Forschung (TMF e.V.) entwickelten Konzepten auf. Eine genauere Beschreibung des Pseudonymisierungsvorgangs wird in projektbezogenen Konzepten festgehalten.

Allen gemeinsam ist die Trennung zwischen personenidentifizierenden Angaben und Studiendaten. Dafür wird für jede eindeutig bestimmte Person eine nicht sprechende Zeichenkette als Personenidentifikationsnummer zufällig erzeugt. Die Personenidentifikationsnummer und die personenidentifizierenden Daten sind weder in den Studiendaten enthalten noch haben andere Einheiten des Datenmanagements Zugriff auf diese Informationen. Davon unabhängig wird für jeden Probanden eine ebenfalls nicht sprechende Zeichenkette als Studiennummer erzeugt, die als Schlüssel zur von den personenidentifizierenden Daten getrennten Speicherung der Studiendaten dient.

Qualitative Studien

Bei der Anonymisierung der erhobenen Interviewdaten werden alle direkten Identifizierungsmerkmale wie genannte Personennamen, Ortsnamen, Straßennamen, Bundesländer, Institutionen (z.B. Firmen,

Schulen, Institute), Berufsangaben, Titel, Bildungsabschlüsse, Zeitangaben, kalendarische Daten, Adressen, Institutionen o.ä. anonymisiert, d.h. durch andere Namen ersetzt, um eine Re-identifizierung der Betroffenen auszuschließen.

Des Weiteren wird zur Gewährleistung der Anonymität der Befragten auf eine komplette Veröffentlichung von Interviews verzichtet. In wissenschaftlichen Veröffentlichungen werden Interviews nur in Ausschnitten zitiert, um gegenüber Dritten sicherzustellen, dass der entstehende Gesamtzusammenhang von Ereignissen nicht zu einer Identifizierung der Person führen kann.

Ist eine weitere Befragung beispielsweise im Rahmen einer Längsschnittuntersuchung geplant, kann im Sinne der Pseudonymisierung eine Liste mit der Zuordnung von personenbezogenen Merkmalen zu datenverwaltungstechnischen Kennziffern erstellt werden. Diese Listen müssen ebenso wie die Adressenlisten getrennt und an gesicherten Speicherorten (netzunabhängiger Rechner) aufbewahrt werden, und nur Befugten zur Verfügung gestellt werden. Einträge personenbezogener Daten in diese Liste dürfen nur erfolgen, wenn durch die Studienteilnehmer/innen eine explizite Einwilligung zu einer erneuten Kontaktierung erfolgt ist.

8. Anonymitäts- und Trennungsgebot

Ergebnisse von Datenerhebungen werden in anonymisierter oder pseudonymisierter Form ausgewertet und nur für Gruppen zusammengefasst dargestellt. Die Gruppen werden so definiert, dass unmittelbare Rückschlüsse auf die Identität zuverlässig ausgeschlossen sind. Schutzwürdige personenbezogene Daten bleiben strikt von den Erhebungsergebnissen getrennt. Es ist gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden.

Darüber hinaus gelten für einzelne Projekte die dafür festgelegten, zusätzlichen Bestimmungen.

9. Datenübermittlung und Weitergabe

Eine Übermittlung schutzwürdiger personenbezogener oder pseudonymisierter Daten kommt nur in jeweils zu vereinbarenden Sonderfällen im Rahmen spezifischer vertraglicher Vereinbarungen und unter Erfüllung gesetzlicher Vorschriften in Frage; sie wird für den Regelfall zuverlässig ausgeschlossen. Soweit eine Übermittlung in Betracht kommt, kann dies nur durch ausgewählte Personen (Projektleiter(innen), Projektkoordinator(innen)) erfolgen. Die Studienteilnehmer*innen müssen in der erfolgten Einwilligungserklärung in die Datenübermittlung eingewilligt haben. Werden Daten außerhalb der Räumlichkeiten der Medizinischen Soziologie weiterverarbeitet (z.B. Transkription von Audiodateien), wird gewährleistet, dass auf die Daten a) direkt über das R-Laufwerk des Servers zugegriffen wird, oder b) in Ausnahmefällen die Dateien auf passwortgesicherten externen Speichergeräten gespeichert und weiterverarbeitet werden. Dabei wird gesichert, dass die Daten während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Ebenfalls ist darauf zu achten, dass die Daten schnellstmöglich auf dem Laufwerk des Instituts für Epidemiologie und Präventivmedizin gespeichert werden. Die Versendung personenbezogener Daten über Email ist untersagt, sofern nicht explizit eine Verschlüsselung der versandten Daten vorgenommen wurde.

10. Auftragskontrolle

Personenbezogene Daten oder pseudonymisierte Daten, die im Auftrag erhoben, verarbeitet oder genutzt werden, werden nur entsprechend den Weisungen des Auftraggebers sowie im Hinblick auf die gesetzlichen Bestimmungen verarbeitet.

11. Dauer der Datenspeicherung

Personenidentifizierende Daten müssen gelöscht werden, wenn sie nicht mehr gebraucht werden, um die spezifische Funktion zu erfüllen (§ 20 BDSG und entsprechende Regelungen in den Datenschutzgesetzen der Länder), spätestens nach Ablauf des Forschungsvorhabens. Pseudonymisiert gespeicherte Befragungs- und Gesundheitsdaten werden aus Gründen guter wissenschaftlicher Praxis nicht vor Abschluss aller wissenschaftlichen Auswertungen gelöscht. Widerruft ein Teilnehmer seine Einwilligung in die Nutzung dieser Daten, werden die Daten gemäß Art. 17 Abs. 1lit. B) DSGVO unverzüglich gelöscht.

12. Verfügbarkeitskontrolle

Personenbezogene oder pseudonymisierte Daten sind gegen zufällige Zerstörung oder Verlust geschützt. Regelmäßig werden vollständige Sicherungen des Servers über das Rechenzentrum erstellt, katalogisiert und unter Verschluss gehalten. Die Serverräume des Rechenzentrums unterliegen den Bestimmungen des Klinikums. Es wird eine redundante Datenhaltung sichergestellt. Zudem besitzen die Serverräume eine Klimaüberwachung, einen Brandschutz, eine USV Kontrolle, ein Notstromaggregat und eine Zugangskontrolle. Es erfolgt ferner eine Datenarchivierung unter Verwendung eines entsprechenden Datenarchivierungssystems.

13. Betroffenenrechte

Die Studienteilnehmer/innen können nach Art. 12 ff. DSGVO ihre Betroffenenrechte beim Verantwortlichen geltend machen. Beispielhaft kann hier das Auskunftsrecht genannt werden: Alle Studienteilnehmer haben das Recht von den Verantwortlichen der jeweiligen Studie eine Auskunft zu erhalten, ob und welche personenbezogenen Daten verarbeitet wurden (DSGVO Art. 15). Darüber hinaus haben alle Teilnehmer/innen die Möglichkeit eine Kopie der personenbezogenen Daten anzufordern.

Darüber hinaus zählen zu den Betroffenenrechten auch das Recht auf Berichtigung der Daten. Der Verarbeitung kann auch widersprochen werden, sie kann eingeschränkt werden und die Daten können auch gelöscht werden, sofern die Daten nicht im Einzelfall aufgrund gesetzlicher Verpflichtungen weiterhin verarbeitet werden müssen.

Zudem kann bei Verstößen auch eine Beschwerde bei der zuständigen Aufsichtsbehörde eingereicht werden.

14. Datenschutzvorkehrungen in Einzelprojekten

In einzelnen Projekten können weitergehende Datenschutzanforderungen angewandt werden, die über die hier beschriebenen Maßnahmen hinausgehen.

15. Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche (xxx) unverzüglich und möglichst binnen 72 Stunden nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde (DSGVO 33). Es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung nicht binnen 72 Stunden, so ist eine Begründung für die Verzögerung beizufügen.