Deutsches Institut für Sucht- und Präventionsforschung, Katholische Hochschule NRW

Datensicherungskonzept für das Forschungsprojekt

"PREPARE (Prevention and Treatment of Substance Use Disorders in Refugees) - Kultursensible digitale Kurzintervention für junge Geflüchtete zur Reduktion von problematischem Alkohol- und Cannabiskonsum - TP3 BePrepared"

Das Deutsche Institut für Sucht- und Präventionsforschung (im Folgenden: DISuP) der Katholischen Hochschule NRW (im Folgenden: KatHO NRW) und das Distributed Artificial Intelligence Laboratory (im Folgenden DAI-Labor) der Technischen Universität Berlin arbeiten neben den allgemeinen Regelungen des Bundesdatenschutzgesetzes auf der Grundlage von internen Regelungen, die auf die umfassende Erfüllung der gesetzlichen Regelungen zum Datenschutz ausgerichtet sind. Die KatHO NRW arbeitet darüber hinaus auch auf der Grundlage des Gesetzes über den Kirchlichen Datenschutz. Für die Datenverarbeitung im Rahmen des Projektes "PREPARE (Prevention and Treatment of Substance Use Disorders in Refugees) - Kultursensible digitale Kurzintervention für junge Geflüchtete zur Reduktion von problematischem Alkohol- und Cannabiskonsum - TP3 BePrepared" (im Folgenden: „BePrepared“) werden zur Sicherung und Schutz von personenbezogenen Daten und von Sozialdaten geeignete räumliche und technische Voraussetzungen nach den Anforderungen des §64 BDSG bzw. §78a SGB X und §§26, 27 KDG geschaffen, welche im Folgenden genannt werden.

1. Anonymitäts- und Trennungsgebot

Das Projektteam arbeitet grundsätzlich nach den geltenden Rechtsvorschriften zum Datenschutz. Zu keinem Zeitpunkt werden einer natürlichen Person einen Datensatz unmittelbar zuordnende Merkmale erhoben (z.B. Name, Adresse, Ausweisnummer, Geburtsdatum, Standort). Das bedeutet, dass das System keine Daten erfasst, die uns oder anderen Nutzern ermöglichen, auf Ihre Identität oder andere persönliche Details zu schließen.

Bei Installation der App wird für jeden Nutzer eine Zufallsnummer generiert, sodass alle Daten unter dieser Zufallsnummer in pseudonymisierter Form erhoben und gespeichert werden (Pseudonymisierung). Eine Anonymisierung erfolgt durch den Nicht-Export dieser Zufallsnummer in den zu auswertenden Datensatz, sodass keinerlei Rückschluss auf den Nutzer möglich ist. Alle Daten werden in anonymisierter Form statistisch ausgewertet und nur für hinreichend große Gruppen zusammenfassend dargestellt. Exporte zu Sicherungskopien erfolgen ebenso nur für hinreichend große Gruppen. Die Gruppen werden so definiert, dass unmittelbare Rückschlüsse auf die Identität Einzelner zuverlässig ausgeschlossen sind.

2. Kontrolle des Zutritts, des Zugangs und des Zugriffs

Für die Büroräume der KatHO NRW und der TU Berlin besteht eine Zutrittskontrolle durch die Ausgabe von Schlüsseln an jeweils berechtigte Personen. Es besteht eine Zugangskontrolle zu PCs als Datenverarbeitungsanlagen durch die Ausgabe von Benutzerkonten mit Passworterzwingung an jeweils berechtigte Personen der KatHO NRW sowie der TU Berlin. Der Zugriff auf den geschützten Server erfolgt durch die Ausgabe von Zugangskonten mit Passworterzwingung an jeweils berechtigte Personen der KatHO NRW sowie der TU Berlin. Der Zugriff auf Sicherungskopien erfolgt über eine Passworterzwingung. Alle Informationen, die das DISuP und das DAI-Labor über den geschützten Server oder Sicherungen erhalten, werden streng vertraulich behandelt.

Die im Projekt „BePrepared“ erhobenen Daten werden im Anschluss im DISuP auf einem geschützten PC verarbeitet. Unbefugte Personen haben zu dem entsprechenden Raum, zu den Programmen/

Datenverarbeitungssystemen sowie zu den Datenbeständen mit schutzwürdigen personenbezogenen Daten oder Sozialdaten keinen Zugang und auch keine Zugriffsmöglichkeit darauf. Zugangsberechtigungen zu PCs sind grundsätzlich passwortgeschützt. Passwörter werden individuell vergeben. Dateinutzungen werden protokolliert und sind jederzeit auf die Einhaltung der Vorgaben überprüfbar. Die Zugriffsberechtigungen auf den Bereich, in dem sich Arbeitsdateien als auch den Bereich, in dem sich die Sicherungen befinden, werden auf den Projektleiter und Mitarbeiterinnen und Mitarbeiter des Forschungsprojekts beschränkt.

In „BePrepared" werden die folgenden Datenverarbeitungsanlagen zu folgenden Zwecken genutzt: das Endgerät (Smartphone) der Studienteilnehmenden zur Erfassung der Daten, ein geschützter Server zur Speicherung und Übertragung der Daten, ein geschützter PC zur Auswertung der Daten sowie lokale Datenträger zur Speicherung von Sicherungskopien. Die Speicherung und Übertragung der Daten auf dem Server erfolgt verschlüsselt mittels SSL. SSL ist eine sichere Transportverschlüsselung.

Die Erfassung der Daten erfolgt ausschließlich über die Nutzung der gesicherten „BePrepared"-Applikation, welche der Studienteilnehmende auf das private Endgerät herunterlädt und installiert. Das DISuP und das DAI-Labor haben über den geschützten Server Zugriff auf Eingaben in Screening und Erhebungen (T(0), T(1), T(2), T(3)), auf die Erhebungen des Nutzungsverhaltens nach Download der gesicherten „BePrepared"-Applikation sowie auf Erklärung und Widerruf des Einverständnisses zur Studienteilnahme und der Nutzungsbedingungen der Applikation.

3. Benutzerkontrolle

Es ist gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Mitarbeiterinnen und Mitarbeiter ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zurückgreifen können. Personenbezogene Daten oder Sozialdaten können bei Verarbeitung, Nutzung und nach der Speicherung durch Mitarbeiterinnen und Mitarbeiter nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

4. Datenträgerkontrolle

Personenbezogene Daten oder Sozialdaten werden ausschließlich innerhalb des DISuP durch die Projektmitglieder unter den beschriebenen Zugangsbeschränkungen gespeichert und verarbeitet. Speicherungen auf anderen lokalen PCs oder eine Datenfernverarbeitung außerhalb der Büroräume der KatHO NRW werden nicht vorgenommen.

5. Eingabekontrolle

Durch die Erfassung der Daten über das Endgerät des Studienteilnehmenden kann aufgrund der Wahrung der Anonymität der Studienteilnehmenden bei Eingabe, Veränderungen oder Entfernung der eigenen Daten über das jeweilige Endgerät keine Benutzeridentifikation und Protokollierung erfolgen. In allen anderen Fällen kann jederzeit überprüft und festgestellt werden, ob und durch wen personenbezogene Daten oder Sozialdaten in Datenvereinbarungssysteme eingegeben, verändert oder entfernt worden sind. Die Überprüfung bzw. Feststellung erfolgt nach einer automatischen und eindeutigen Benutzeridentifikation und einer automatischen Protokollierung. Die Löschung personenbezogener Daten oder von Sozialdaten nach Ablauf des Forschungsprojektes wird ebenso protokolliert.

6. Weitergabekontrolle

Während der Laufzeit des Projektes werden die Arbeitsdateien auf dem im Rahmen des Projekts „BePrepared" genutzten gesicherten Server gesichert. Es ist zu jedem Zeitpunkt garantiert, dass

personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden und kontrollierbar, an welcher Stelle Daten weitergereicht wurden.

7. Verfügbarkeitskontrolle

Die im Rahmen des Forschungsprojektes „BePrepared“ anfallenden personenbezogenen Daten und Sozialdaten werden gegen Zerstörung oder gegen Datenverlust durch verschlüsselte Sicherungskopien geschützt. Diese Sicherung der Arbeitsdateien wird auf gesonderten lokalen Datenträgern erstellt und in einem verschließbaren Schrank aufbewahrt. Dieser Schrank befindet sich in einem anderen Raum als die Datenverarbeitungsgeräte, auf denen die Arbeitsdateien zur Verarbeitung gespeichert sind. Es gelten die unter Punkt 2. genannten Zugangsregeln.

8. Datentrennungskontrolle

Es ist sichergestellt, dass die zu einem unterschiedlichen Zweck erhobenen Daten getrennt behandelt werden.

9. Zugriffsberechtigte Personen

Es ist ausschließlich dem Projektleiter und den dazu autorisierten Projektmitarbeiterinnen und Projektmitarbeiter des DISuP sowie des DAI-Labor gestattet, Sozialdaten zu verarbeiten und Kenntnis von ihnen zu erhalten.
Diese Personen sind:
Prof. Dr. Michael Klein, Projektleiter, Mail: mikle@katho-nrw.de, Tel.: 0221-7757-156
Prof. Dr. Dr. h.c. Sahin Albayrak, Projektleiter, Mail:
Vera Kölligan, Wissenschaftliche Mitarbeiterin, Mail: v.koelligan@katho-nrw.de, Tel.: 0221-7757- 168
Laura Fischer, Wissenschaftliche Mitarbeiterin, Mail: l.fischer@katho-nrw.de, Tel.: 0221-7757-172
Nizar Ben-Sassi, Wissenschaftlicher Mitarbeiter, Mail: nizar.ben-sassi@gt-arc.com
Paul Zernicke, Wissenschaftlicher Mitarbeiter, Mail: paul.zernicke@dai-labor.de

10. Abweichungen von den Datenschutzbestimmungen

Schwerwiegende unerwünschte Ereignisse (SAE, engl.: „serious adverse event“) werden registriert. Ein medizinischer Fragebogen während des Screenings wird genutzt um gesundheitsbezogene Kontraindikationen für die Nutzung der Applikation (Schwangerschaft, Herzerkrankung, Einnahme von Medikamenten, bestehende Substanzabhängigkeit) werden erhoben und es ist garantiert, dass betroffene Teilnehmenden eine spezifische, automatische Rückmeldung zu der Problematik über das Endgerät gegeben wird. Im Kontext der Studie wird kein persönlicher Kontakt zu Studienteilnehmenden bestehen und von den Datenschutzbestimmungen nicht abgewichen.

Köln, 09.01.2021