German Institute for Addiction and Prevention Research, Catholic University NRW

Data security concept for the research project

"PREPARE (Prevention and Treatment of Substance Use Disorders in Refugees) - Culturally sensitive digital brief intervention for young refugees with problematic use of alcohol and cannabis - TP3 BePrepared"

The German Institute for Addiction and Prevention Research (hereinafter: DISuP) of the Catholic University of Applied Sciences NRW (hereinafter: KatHO NRW) and the Distributed Artificial Intelligence Laboratory (hereinafter: DAI-Labor) of the Technical University of Berlin work, in addition to the general regulations of the Federal Data Protection Act, on the basis of internal regulations that are geared towards comprehensive compliance with the legal regulations on data protection. The KatHO NRW also operates on the basis of the Church Data Protection Act. For data processing within the framework of the project "PREPARE (Prevention and Treatment of Substance Use Disorders in Refugees) - Culturally Sensitive Digital Brief Intervention for Young Refugees with Problematic Use of Alcohol and Cannabis - TP3 BePrepared" (hereinafter: "BePrepared"), suitable spatial and technical conditions are created to secure and protect personal data and social data in accordance with the requirements of §64 BDSG or §78a SGB X and §§26, 27 KDG, which are stated below.

1. Anonymity and separation requirement

As a matter of principle, the project team works in accordance with the applicable legal provisions on data protection. At no time are characteristics directly assigning a data record to a natural person collected (e.g. name, address, ID number, date of birth, location). This means that the system does not collect any data that allows us or other users to infer your identity or other personal details.

When the app is installed, a random number is generated for each user so that all data under this random number is collected and stored in pseudonymized form (pseudonymization). Anonymization is achieved by not exporting this random number to the data set to be analyzed, so that no inference can be made about the user. All data is analyzed statistically in anonymized form and only summarized for sufficiently large groups. Exports to backup copies are also only made for sufficiently large groups. The groups are defined in such a way that direct conclusions about the identity of individuals are reliably excluded.

2. Control of access, entry and access control

For the offices of the KatHO NRW and the TU Berlin there is an access control by issuing keys to authorized persons. There is an access control to PCs as data processing systems by issuing user accounts with forced passwords to authorized persons of KatHO NRW and TU Berlin. Access to the protected server is controlled by issuing access accounts with password enforcement to authorized persons of the KatHO NRW and the TU Berlin. The access to backup copies is done by password enforcement. All information received by DISuP and DAI-Labor via the protected server or backups will be kept strictly confidential.

The data collected in the "BePrepared" project are subsequently processed in the DISuP on a protected computer. Unauthorized persons have no access to the room in question, to the programs/data processing systems as well as to the data files containing personal data or social data worthy of protection. Access authorizations to PCs are always password-protected. Passwords are assigned individually. File usage is logged and can be checked for compliance at any time. Access

rights to the area where working files are located as well as to the area where backups are located are restricted to the project manager and employees of the research project.

In "BePrepared", the following data processing equipment will be used for the following purposes: the end device (smartphone) of the study participants to collect the data, a protected server to store and transfer the data, a protected computer to analyze the data, and local data carriers to store backups. The storage and transmission of data on the server is encrypted using SSL. SSL is a secure transport encryption.

Data is collected exclusively through the use of the secure "BePrepared" application, which the study participant downloads and installs on the private device. The DISuP and DAI lab have access via the protected server to screenings and surveys entries (T(0), T(1), T(2), T(3)), usage behavior surveys after downloading the secure "BePrepared" application, as well as declaration and revocation of consent to study participation and terms of use of the application.

3. User control

It is ensured that employees authorized to use a data processing system can only access the data subject to their access authorization. Personal data or social data cannot be read, copied, modified or removed by employees without authorization during processing, use or after storage.

4. Data carrier control

Personal data or social data are stored and processed exclusively within the DISuP by project members under the described access restrictions. Storage on other local computers or remote data processing outside the offices of the KatHO NRW will not be undertaken.

5. Input control

Due to the preservation of the anonymity of the study participants, the collection of data via the end device of the study participant means that no user identification and logging can take place when entering, changing or removing one's own data via the respective end device. In all other cases, it can be checked and determined at any time whether and by whom personal data or social data have been entered, changed or removed in data agreement systems. The verification or determination is carried out after automatic and unique user identification and automatic logging. The deletion of personal data or social data after the end of the research project is also logged.

6. Forwarding control

During the duration of the project, the working files are backed up on the secured server used in the "BePrepared" project. It is guaranteed at all times that personal data are not read, copied, changed or removed without authorization and it is controllable at which point data have been passed on.

7. Availability control

The personal data and social data generated in the course of the "BePrepared" research project are protected against destruction or against data loss by encrypted backup copies. This backup of the working files is created on separate local data carriers and stored in a lockable cabinet. This cabinet is located in a different room from the data processing equipment on which the work files are stored for processing. The access rules stated in bullet point 2. above shall apply.

8. Data separation control

It is ensured that the data collected for a different purpose are treated separately.

9. Persons authorized to access

Only the project manager and authorized project staff of DISuP and DAI-Labor are allowed to process and gain knowledge of social data.

These persons are:

Prof. Dr. Michael Klein, Project Manager, Mail: mikle@katho-nrw.de, Tel.: 0221-7757-156

Prof. Dr. Dr. h.c. Sahin Albayrak, Project Manager, Mail:

Vera Kölligan, Research Assistant, Mail: v.koelligan@katho-nrw.de, Tel.: 0221-7757- 168

Laura Fischer, Research Associate, Mail: l.fischer@katho-nrw.de, Tel.: 0221-7757-172

Nizar Ben-Sassi, Research Associate, Mail: nizar.ben-sassi@gt-arc.com

Paul Zernicke, Research Associate, Mail: paul.zernicke@dai-labor.de

10. Deviations from the data protection regulations

Serious adverse events (SAEs) are recorded. A medical questionnaire during screening will be used to collect health-related contraindications to the use of the application (pregnancy, heart disease, taking medication, existing substance dependence) and it is guaranteed that affected participants will be given specific, automatic feedback on the issue via the terminal. In the context of the study, there will be no personal contact with study participants and there will be no deviation from data protection regulations.

Cologne, 09.01.2021