



STRENGTHS DATA PROTECTION POLICY

DELIVERABLE 9.2



This project has received funding from the European Union's Horizon 2020 Research and Innovation programme Societal Challenges under Grant Agreement No 733337.

About this document

Work Package in charge: WP9 Ethics Requirements

Delivery date of this deliverable: June 29, 2017

Dissemination level: CO (only for members of the Consortium including the Commission Services).

Project acronym: STRENGTHS (Syrian REfuGees MeNTal Health Care Systems)

Funding organisation: EU Horizon2020 – Research and Innovation Action

EU Project number: 733337

Lead author:

Marit Sijbrandij, VU University Amsterdam, Faculty of Behavioural and Movement Sciences, Department of Clinical, Neuro- and Developmental Psychology, the Netherlands

Other contributing partners:

Freie Universität Berlin, Christine Knaevelsrud, Sebastian Burchert

International Medical Corps, Inka Weissbecker, Claire Whitney

Istanbul Sehir Universitesi, Ceren Acarturk

KIT, Egbert Sondorp

London School of Economics and Political Science, David McDaid, A-La Park

London School of Hygiene and Tropical Medicine, Bayard Roberts

University Hospital Zurich, Naser Morina, Matthis Schick, Monique Pfaltz, Ulrich Schnyder

University of New South Wales, Richard Bryant

War Child, Mark Jordans, Frederik Steen

Danish Red Cross, Martha Bird, Pernille Hansen, Louise Juul Hansen

Contacts: info@strengths-project.eu

Visit us on: www.strengths-project.eu

Table of content

About this document	2
List of abbreviations and acronyms	4
Definitions	5
1. STRENGTHS Data Protection Policy	6
1.1. Involvement and responsibilities of partners	6
1.2. Data protection	6
1.3. Transfer of data	7
1.4. Informed Consent.....	7
2. Overview of local STRENGTHS datasets to be collected	8
2.1. Datasets collected in WP1.....	8
2.2. Datasets collected in WP2.....	8
2.3. Datasets collected in WP3.....	9
2.4. Datasets collected in WP4.....	12
2.5. Datasets collected in WP5.....	16
2.6. Datasets collected in WP6.....	21
2.7. Datasets collected in WP7	23
2.8. Datasets collected in WP8.....	24
3. STRENGTHS partners involved in STRENGTHS Data Management.....	25
Appendix: Data Protection Labels	31

List of abbreviations and acronyms

DFG	The Germany Research Foundation
DMPP	Data Management and Protection Plan
DRC	Reference Centre for Psychosocial Support/Danish Red Cross
FUB	Freie Universitaet Berlin
EASE	Early Adolescent Skills for Emotions
IMC	International Medical Corps UK LBG
ISU	İstanbul Sehir Universitesi
IPSY	I-Psy Midden en Noord Nederland (IPSY)
KIT	The Royal Tropical Institute
LSE	London School of Economics and Political Science
LSHTM	London School of Hygiene and Tropical Medicine
N/A	Not Applicable
PM+	Problem Management Plus
RASASA	Multeciler Ve Siginmacilar Yardimlasma Ve Day Anisma Dernegi
STRENGTHS	Syrian REfuGees MeNTal HeAlTH Care Systems
UNSW	University of New South Wales
UZH	Universität Zürich
VUA	Vrije Universiteit Amsterdam
WCH	War Child Holland
WHO	World Health Organization
WMO	Dutch Medical Research Involving Human Subjects Act
WP	Work Package
WTF	Stichting War Trauma Foundation

Definitions¹

Controller:

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Personal data:

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Primary data:

Data observed or collected directly from participants and first-hand experience.

Processing:

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pseudonymous data

Pseudonymous data means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Secondary data:

Data collected in the past by other parties.

Sensitive data:

Sensitive personal data are defined as data on a person's race, ethnic origin, political opinion, religious or similar beliefs, trade union membership, physical or mental health condition, sexual life, commission or alleged commission of an offence, proceedings for an offence (alleged to have been) committed, disposal of such proceedings or the sentence of any court in such proceedings.

¹Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (2016).

1. STRENGTHS Data Protection Policy

The Data Protection Policy describes the data protection measures that will be implemented in the institution in which the research will be carried out. The Data Protection Policy is part of the overall STRENGTHS DMPP (D1.1), but is also a separate deliverable for Work Package 9 (Deliverable 9.1).

It includes the organizational and technical details about data collection, data storage, retention, destruction, privacy and confidentiality. It also includes details of transfer of data.

Within each institution where data are collected, analyzed or stored, a local data protection officer has been identified and has confirmed that all EU and national legislation is carried out with regard to the processing of personal data (see Appendix).

1.1. Involvement and responsibilities of partners

All STRENGTHS Consortium partners will be responsible for compliance to the DMPP, in particular for the data management of their own dataset. The datasets that will be collected under responsibility of these partners are outlined in Chapter 3.

The following STRENGTHS partners will be directly involved in the STRENGTHS data collection, by either collecting, storing, or analysing STRENGTHS data: VUA (The Netherlands, coordinator), DRC (Denmark), FUB (Germany), IMC (London), KIT (The Netherlands), LSE (United Kingdom), LSHTM (United Kingdom), WCH (the Netherlands), ISU (Turkey), UNSW (Australia), and UZH (Switzerland). Partners IPSY (The Netherlands) and RASASA (Turkey) will have a limited role in data collection. Their role will be to ask permission to their clients to be informed about the trials in the Netherlands and Turkey, respectively. Partners UNHCR (Switzerland) and WTF (The Netherlands) do not handle, process or disseminate any personal or research data since their central tasks are in WP8 (Dissemination).

The VUA Project office and STRENGTHS Safety Board are also central players in the implementation of the DMP and will track the compliance of the rules agreed upon.

1.2. Data protection

STRENGTHS involves the collection and use of personal information from Syrian refugees with symptoms of psychological distress and impaired functioning. This will include individual data on psychological distress, psychosocial functioning, quality of life, health costs, and selected demographic information such as age, gender, community of origin, and education level. The data will be collected through interviews and questionnaires. Data on health care systems from relevant stakeholders will also be included via questionnaires and interviews. Data will also be recorded on project partners implementation related activities.

Procedures for the collection and storage of personal data will comply with relevant European regulations and directives. This will include the adherence to the *Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the*

*processing of personal data and on the free movement of such data.*² In addition, partners will adhere to all relevant national legislation and regulations and the specific regulations of the institutions in which the trials will take place. These regulations are described in Chapter 6 for each of the partners that collect data. In cases where local regulations on privacy or data protection are absent, partners will follow the EU regulations. In case they deviate from EU standards, partners will adopt the criteria providing the strongest protection for trial participants.

In order to safeguard the confidentiality of the participants' personal information, the data will be stored in a record that will be kept locked in the lead institutions of the relevant study. Only authorized research personnel will have access to this personal information. Each participant will be given a numerical code to replace identifying information and ensure pseudonymity. Lists with names and numbers will be kept separate from the dataset and will be safely stored. Access to the data files will be restricted to researchers and clinicians involved in the studies, and the staff involved will be required to sign a confidentiality agreement. After collection, data will be electronically encrypted using appropriate software. Data will only be reported in aggregated form and will never highlight a single individual's data. Appropriate measures will be taken to prevent unauthorized use of study information. Pseudonymous data will only be shared within the STRENGTHS Consortium for scientific collaboration.

1.3. Transfer of data

Only pseudonymised data will be transferred between partners.

Data will only be transferred if the data subject has provided informed consent for data transfer (see also 1.7). In addition, the supplying partner and the receiving partner have agreed on a separate bilateral or multilateral data transfer agreement specifying the conditions of such transfer and processing of personal data. The Consortium Agreement provides a template for a data transfer agreement between partners. In case the receiving partner resides in a country, which does not provide an adequate level of data protection, in particular due to the absence of legislation that guarantees adequate protection, the data transfer will be based on sufficient safeguards.

1.4. Informed Consent

The principles of the Declaration of Helsinki³ will be respected. Ethics approval will be gained from authorized Ethics Review Boards in countries that will be collecting data (both in the EU and in the third countries Switzerland, Lebanon, Jordan, and Egypt). No data will be collected or used without the explicit informed consent of the participants or their legal guardians. Participants can withdraw at any point without any disadvantage. As part of the informed consent procedure, informed consent for data transfer to other parties, and long-term preservation will also be asked. The information sheet and informed consent both include a section on the collection and storage of personal data in databases, a statement regarding the period of storage of data, transfer of data and possible use for future studies. The information in the information sheet will also be put on the STRENGTHS website (www.strengths-project.eu)

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (2016).

³ World Medical Organisation. *Declaration of Helsinki*. 2013.

2. Overview of local STRENGTHS datasets to be collected

Tables 4.1 to 4.8 provide an overview of all research data sets that will be collected during the course of STRENGTHS across all work packages.

2.1. Datasets collected in WP1

WP1 Management and overall coordination	
Data set reference and name	WP1 will not generate data sets

2.2. Datasets collected in WP2

WP2 Health Systems Evaluation	
Data set reference and name	WP2 Health Systems Evaluation
STRENGTHS partner	LSHTM (Dr. Bayard Roberts; bayard.roberts@lshtm.ac.uk) KIT (Dr. Egbert Sondorp, e.sondorp@kit.nl)
Countries where data are gathered	All project countries
Purpose of the data collection	To analyze the responsiveness of health systems to the scaling-up PM+ intervention for Syrian refugees
Type, format and size of data	<ol style="list-style-type: none"> 1. Qualitative data from approximately 200 semi-structured interviews. Data contain information about respondents (e.g. position held, gender, and approximate age). Respondents include health care users, health service providers, health experts. No personal identifiers will be recorded. Estimated file size 10GB 2. Audiotapes of approximately 24 focus group interviews with health care users and providers. No personal information contained. Estimated file size 2 GB. 3. SPSS data files containing quantitative data from cross-sectional surveys in approx. 2400 participants. Data files contain information about Syrian refugee mental health outcomes and utilization of services and basic demographic and socio-economic data (age, gender, education level, income-level). No personal identifiers. Data will be stored pseudonymous (under participant number, identifying characteristics such as names will be removed). Estimated size: 6 MB. 4. A list of participant numbers, names and birth dates that matches SPSS data files under 1. (personal data). Estimated size: 1 MB 5. Pen-and-paper surveys of approx. 2400 participants. Data will be stored pseudonymous (under participant number).
Data Sharing	Data under 1. and 3. will be shared with LSE for re-use in WP7.

Reuse of existing data and origin of existing data	Not applicable
Pseudonymous data to be stored, storing and transfer locations	Pseudonymous data will be stored at the London School of Hygiene and Tropical Medicine as KIT staff involved (Egbert Sondorp) have access to LSHTM encrypted data storage. Pseudonymous data will be transferred from data collection partners to the London School of Hygiene and Tropical Medicine.
Archiving and preservation of sensitive data	No sensitive data will be collected.
Estimated costs of data storage	Zero cost to STRENGTHS study.
Data security	
Use of secure or encrypted communication methods to transfer data	Data will be encrypted using Filr software.
Duration of data storage	Paper-based datasets will be securely stored for 5 years and then destroyed. Digital datasets will be securely stored for 10 years and then destroyed.

2.3. Datasets collected in WP3

WP3 Adaptation	
Data set reference and name	WP3 Cultural adaptation
STRENGTHS partners	Lead: DRC (Martha Bird) Other partners: IMC (Claire Whitney), WCH (Mark Jordans), VUA (Marit Sijbrandij), ISU (Ceren Acarturk), UZH (Naser Morina), FUB (Christine Knaevelsrud).
Countries where data are gathered	Jordan, Lebanon, the Netherlands, Turkey, Switzerland, Germany, Egypt, Sweden.
Purpose of the data collection	Cultural adaptation of the different versions of the scalable WHO programmes including cross-cultural analysis and analysis across PM+ types
Type, format and size of data	<ol style="list-style-type: none"> 1. Audiotapes (mp3 files) of free listing interviews, key informant interviews and focus group discussions with healthy Syrian refugees and local mental health professionals and policy makers in refugee mental health care in Jordan, Lebanon, the Netherlands, Switzerland, Germany, Egypt, Sweden. They will be destroyed after transcriptions are made. Estimated size: 24GB. Note: in Turkey, no audio recordings will be made. 2. Pseudonymous transcriptions and translations of audiotapes of key informant interviews and focus group discussions (word documents). Estimated size: 40MB 3. A dataset in Excel or Nvivo software with pseudonymous scored data of the interviews. Estimated size: 40MB 4. Explanatory files (codebooks/log files) will be saved as excel, SPSS, word or PDF files. Estimated size: 16MB 5. Paper- and-pencil informed consent forms with name and signatures

	<p>(word documents) in Jordan, Lebanon, the Netherlands, Turkey, Switzerland, Germany, Egypt, Sweden.</p> <p>6. Audiotapes (mp3 files) of cognitive interviews, focus group discussions and adaptation workshops. They will be destroyed after transcriptions/list of recommendations are made. Estimated size: 3GB. Note: in Turkey, no audio recordings will be made.</p> <p>7. Pseudonymous transcriptions and translations of audiotapes of cognitive interviews, focus group discussions (word documents). Estimated size: 5MB (focus group interviews and audio recordings)</p> <p>8. A dataset in Excel or Nvivo software with pseudonymous scored data of the cognitive interviews and focus group discussions. Estimated size: 5MB</p> <p>9. A word file per PM+ material with minutes of the workshop and the recommendations for the cultural adaption.</p>
Data Sharing	IMC, WCH, VUA, ISU, UZH, and FUB will share data collected in the project countries described under 2. and 7. with DRC. DRC will merge and analyze qualitative data. IMC will also share data with UNSW.
Reuse of existing data and origin of existing data	Not applicable
Pseudonymous data to be stored, storing and transfer locations	<p>DRC: All data in the data set will be stored pseudonymous, and they will be available only to the DRC research team members.</p> <p>All pseudonymous data to be stored at DRC, are stored on the DRC internal secure server.</p> <p>IMC: IMC keeps client files stored confidentially in locked filing cabinets at the field level in Amman(Jordan). All electronic data in the data set will be stored pseudonymous on an internal secure server at the IMC office in Amman (Jordan), and they will be available only to the IMC research team members.</p> <p>All pseudonymous data to be stored at DRC, on the DRC internal secure server.</p> <p>WCH: All data is de-identified with unique numeric identifiers. Codes for re-identifying purposes to permit follow-up of participants will be separately stored in locked premises at the War Child Holland Lebanon Office by the Research Coordinator.</p> <p>All data will be entered and downloaded electronically on tablets. These data will be pseudonymised. The electronic files will be stored on a password protected server, cloud based in West-Europe (Azure, by Microsoft) on a password protected and encrypted platform only accessible for the primary investigators at War Child in Lebanon. On this drive a separate folder for PM+ exists and folders are made for every phase of the study (e.g. formative, pilot, evaluation etc.). The original datasets will be uploaded on one part of the Server , accessible by the Research Coordinator of the Lebanon country Office and will be uploaded by the team in Head Office of War Child Holland. They will store it on a separate folder on the server (only accessible by primary and co-investigators) before data transformation and analysis will take place.</p> <p>VUA: All data in the data set will be stored pseudonymous, and they will be available only to the VUA research team members.</p> <p>All pseudonymous data to be stored at the VU, will be stored in a data</p>

	<p>repository named DataverseNL. DataverseNL is an online platform that can be used to share and publish research data in a (semi-) open environment. It is possible to link to a DataverseNL dataset in publications.</p> <p>UZH: All data in the data set will be stored pseudonymous at a research server of the University Hospital Zurich and they will be available only to the USZ/UZH research team members.</p> <p>ISU: All pseudonymous data to be stored at ŞEHİR, will be stored in a data repository named ŞEHİR Academic Repository (DSpace) is an online platform that can be used to share and publish research data in a (semi-) open environment. It is possible to link to a ŞEHİR Academic Repository (DSpace) dataset in publications.</p> <p>FUB: All data will be encrypted and stored pseudonymous. Data will be transferred to DRC via a secure email system with OTP encryption.</p>
Archiving and preservation of sensitive data	No sensitive data will be stored.
Estimated costs of data storage	There are no costs involved in data management during the course of STRENGTHS for partners, since partners have sufficient capacity for data storage on their servers.
Data security	
Use of secure or encrypted communication methods to transfer data	<p>DRC: Secure data transfer is achieved through the DRC secure email setup, which encrypts the email and data that is being transferred and establishes a secure channel of communication between @rodekors.dk emails and other mailbox systems. This setup will allow you to send data to and from DRC via email in a secure way as an attachment to an email. DRC internal emailing (@rodekors.dk mailboxes) is also safeguarded, meaning that DRC staff can send data between one another in a secure manner regardless of locations. Personal laptops are password protected, and run Window10 with Bitlocker device encryption.</p> <p>IMC: Data will be encrypted using encryption software (software will be determined).</p> <p>WCH: Data will be encrypted using encryption software (software will be determined).</p> <p>VUA: Data will be encrypted using the encryption software that is used in the Surfdrive cloud service.</p> <p>ISU: VeraCrypt encryption software will be used</p> <p>UZH: VeraCrypt encryption software will be used</p> <p>FUB: VeraCrypt encryption will be used</p>
Duration of data storage	<p>DRC: No longer than project closure, 31/12/2021</p> <p>IMC: No longer than project closure</p> <p>WCH: 7 years</p> <p>VUA: 5 years</p> <p>ISU: 5 years</p> <p>UZH: 10 years</p> <p>FUB: 10 years</p>

2.4. Datasets collected in WP4

WP4 Refugee Settlement and Camp Implementation	
Data set reference and name	WP4 Refugee Settlement Implementation-Jordan
STRENGTHS partner	UNSW (prof Richard Bryant; r.bryant@unsw.edu.au) Local research partner will also be involved. This partner will be subcontracted during the course of STRENGTHS.
Countries where data are gathered	Jordan
Purpose of the data collection	Collection of assessment and outcome data related to psychological interventions implemented in Syrian refugees located in refugee settlements in Jordan (WP4)
Type, format and size of data	<p>Data are self-reported data of psychological responses in Syrian adult refugees and their children (approximately 2000 respondents).</p> <ol style="list-style-type: none"> 1. SPSS or Excel data files containing screening data and clinical self-reported data of psychological responses in Syrian adult refugees and their children in Jordan. Data files contain information about demographic characteristics (age, education, etc.), symptoms of psychological distress, disability, anxiety, depression, posttraumatic stress-symptoms and health costs. Data will be stored pseudonymous (under participant number, identifying characteristics such as names will be removed). Estimated size: 10 MB 2. A list of participant numbers, names and birth dates that matches that SPSS data files under 1. (personal data). Estimated size: 1 MB 3. Surveys of interviews and questionnaires containing screening data and clinical outcome data from Syrian refugees participating in the STRENGTHS implementation studies in WP4 in Jordan will be collected on electronic tablets and data automatically downloaded. Questionnaires contain information about demographic characteristics (age, education, etc.), symptoms of psychological distress, disability, anxiety, depression, posttraumatic stress-symptoms, health service utilisation and health service costs. Data will be stored pseudonymous (under participant number, identifying characteristics such as names will be removed). 4. Approx. 1500 paper- and-pencil informed consent forms with name and signature (word documents). 5. Qualitative interviews in study participants and key informants after completion of exploratory trial and definitive trials: 1hr per interview (\pm300Mb).
Data Sharing	<p>Data under 1. (see above) will be merged with similar data collected in WP4, 5 and 6. This merged dataset will be shared with LSE and VUA for re-use in WP7. In addition, the dataset will be made available upon request for STRENGTHS partners who are interested to answer additional scientific research questions.</p> <p>Data under 5. (see above) will be shared with LSHTM and KIT to inform the rapid health systems assessments.</p>
Reuse of existing data and origin of existing data	Not applicable
Pseudonymous data to be	All data is de-identified with unique numeric identifiers. Codes for re-

stored, storing and transfer locations	<p>identifying purposes to permit follow-up of participants will be separately stored in locked premises in the headquarters of the local research partner (to be determined).</p> <p>All data will be entered and downloaded electronically on tablets. These data will be de-identified.</p> <p>Deidentified data will be securely stored on a secure server at UNSW. The electronic files will be stored on a password protected server (Azure, by Microsoft) on a password protected and encrypted platform. On this drive a separate folder for PM+ exists and folders are made for every phase of the study (e.g. formative, pilot, evaluation etc.).</p> <p>All dataset will be pseudonymized and stored on the server, only accessible by primary investigators at UNSW in Sydney and at War Child in Jordan.</p>
Archiving and preservation of sensitive data	<p>During the course of STRENGTHS, this list will be stored independently of responses by ensuring all responses are deidentified and linked with names and identifying information in a separate file. The file linking identifying information with unique participant Identification Numbers will be stored at UNSW in locked premises.</p> <p>After completion of STRENGTHS, sensitive data will be stored in electronically on a secure IT network hosted at UNSW. Access will be restricted to research staff directly involved in the study.</p>
Estimated costs of data storage	Data storage will be stored electronically on UNSW server that is provided by UNSW, and therefore there is no cost to STRENGTHS.
Data security	
Use of secure or encrypted communication methods to transfer data	Data will be encrypted using Azure Disk Encryption.
Duration of data storage	Data will be stored for the 7 years following the completion of STRENGTHS.

Data set reference and name	WP4 Refugee Settlement Implementation-Lebanon
STRENGTHS partner	WCH (Mark Jordans; Mark.Jordans@warchild.nl)
Countries where data are gathered	Lebanon
Purpose of the data collection	To inform the process of comprehensive adaptation of the scalable WHO Early Adolescent Skills for Emotions (EASE) programme towards the Lebanese context and to evaluate the effectiveness of EASE to reduce psychological distress in young adolescent Syrian refugees in different communities in Lebanon affected by adversity (WP4).
Type, format and size of data	<p>Data are self-reported data of psychological responses in Syrian children and their parents (approximately 1500 respondents).</p> <p>1. SPSS or Excel data files containing screening data and clinical self-reported data of psychological responses in Syrian adult refugees and their children in Lebanon. Data files contain information about demographic characteristics (age, education, etc.), symptoms of psychological distress, disability, anxiety, depression, posttraumatic stress-symptoms, health service use and health costs. Data will be stored pseudonymous (under participant number, identifying characteristics such as names will be removed). Estimated size: 10 MB</p> <p>2. A list of participant numbers, names and birth dates that matches</p>

	<p>that SPSS data files under 1. (personal data). Estimated size: 1 MB</p> <p>3. Surveys of interviews and questionnaires containing screening data and clinical outcome data from young adolescents Syrian refugees participating in the STRENGTHS implementation studies in WP4 in Lebanon will be collected on electronic tablets and data automatically downloaded. Questionnaires contain information about demographic characteristics (age, education, etc.), symptoms of psychological distress, disability, anxiety, depression, posttraumatic stress-symptoms and health costs. Data will be stored pseudonymous (under participant number, identifying characteristics such as names will be removed).</p> <p>4. Approx. 1500 paper- and-pencil informed consent forms, including part with assent from children, with name and signature</p> <p>5. Qualitative interviews in study participants and key informants after completion of exploratory trial and definitive trials: 1hr per interview ($\pm 300\text{Mb}$).</p>
Data Sharing	<p>Pseudonymous qualitative transcriptions and datasets described under 5) (see above) will be merged with similar data collected in WP4, 5 and 6. This merged dataset will be shared with LSHTM and KIT in WP2.</p> <p>Pseudonymous quantitative datasets described under 1) will be merged with similar data collected in WP4, 5 and 6 and shared with LSE and VUA for re-use in WP7. In addition, the dataset will be made available upon request for STRENGTHS partners who are interested to answer additional scientific research questions.</p>
Reuse of existing data and origin of existing data	Not applicable
Pseudonymous data to be stored, storing and transfer locations	<p>All data is de-identified with unique numeric identifiers. Codes for re-identifying purposes to permit follow-up of participants will be separately stored in locked premises at the War Child Holland Lebanon Office by the Research Coordinator.</p> <p>All data will be entered and downloaded electronically on tablets. These data will be pseudonymised. The electronic files will be stored on a password protected server, cloud based in West-Europe (Azure, by Microsoft) on a password protected and encrypted platform only accessible for the primary investigators at War Child in Lebanon. On this drive a separate folder for PM+ exists and folders are made for every phase of the study (e.g. formative, pilot, evaluation etc.).</p> <p>The original datasets will be uploaded on one part of the Server, accessible by the Research Coordinator of the Lebanon country Office and will be uploaded by the team in Head Office of War Child Holland. They will store it on a separate folder on the server (only accessible by primary and co-investigators) before data transformation and analysis will take place.</p>
Archiving and preservation of sensitive data	<p>The hardcopy file linking identifying information with unique participant Identification numbers will be stored in locked premises. The digital version of this document will be stored on the Azure server, separately from the Research dataset.</p> <p>Access will be restricted to research staff directly involved in the study. Datasets containing sensitive data will only be transferred between the Lebanon Country Office and Head Office of War Child Holland, where the storage on the server will take place. Datasets containing sensitive</p>

	data will only be transferred between the Lebanon Country Office and Head Office of War Child Holland, where the storage on the server will take place.
Estimated costs of data storage	Data storage will be stored electronically on War Child Holland's server, and therefore there is no cost to STRENGTHS.
Data security	
Use of secure or encrypted communication methods to transfer data	Internally, WC data will be shared between Lebanon and Head Office in the Netherlands, by sharing via the Azure Server. Externally, data will be transferred via an encrypted local secured FTP server, which is part of the WCH Head Office ICT Infrastructure. Data will be encrypted using encryption software (software will be determined).
Duration of data storage	Data will be stored for 7 years following completion of STRENGTHS.

Data set reference and name	WP4 Refugee Camp Implementation-Jordan
STRENGTHS partner	UNSW (prof Richard Bryant; r.bryant@unsw.edu.au) and IMC (Inka Weissbecker and Claire Whitney)
Countries where data are gathered	Jordan
Purpose of the data collection	To inform the process of comprehensive adaptation of the scalable WHO PM+ programmes for implementation in community and camp settings in Jordan and to evaluate implementation of the PM+ programmes in refugee camps in Jordan (WP4).
Type, format and size of data	Data are self-reported data of psychological responses in Syrian adult refugees and their children (approximately 2000 respondents). 1. SPSS or Excel data files containing screening data and clinical self-reported data of psychological responses in Syrian adult refugees and their children in Jordan. Data files contain information about demographic characteristics (age, education, etc.), symptoms of psychological distress, disability, anxiety, depression, posttraumatic stress-symptoms and health costs. Data will be stored pseudonymous (under participant number, identifying characteristics such as names will be removed). Estimated size: 10 MB 2. A list of participant numbers, names and birth dates that matches that SPSS data files under 1. (personal data). Estimated size: 1 MB 3. Surveys of interviews and questionnaires containing screening data and clinical outcome data from Syrian refugees participating in the STRENGTHS implementation studies in WP4 in Jordan will be collected on electronic tablets and data automatically downloaded. Questionnaires contain information about demographic characteristics (age, education, etc.), symptoms of psychological distress, disability, anxiety, depression, posttraumatic stress-symptoms, health service use and health costs. Data will be stored pseudonymous (under participant number, identifying characteristics such as names will be removed). 4. Approx. 1500 paper- and-pencil informed consent forms with name and signature (word documents). 5. Qualitative interviews in study participants and key informants after completion of exploratory trial and definitive trials: 1hr per interview (\pm 300Mb).
Data Sharing	Pseudonymous qualitative transcriptions and datasets described under

	5) (see above) will be merged with similar data collected in WP4, 5 and 6. This merged dataset will be shared with LSHTM and KIT in WP2. Pseudonymous quantitative datasets described under 1) will be merged with similar data collected in WP4, 5 and 6 and shared with LSE and VUA for re-use in WP7. In addition, the dataset will be made available upon request for STRENGTHS partners who are interested to answer additional scientific research questions.
Reuse of existing data and origin of existing data	Not applicable
Pseudonymous data to be stored, storing and transfer locations	<p>All data is de-identified with unique numeric identifiers. Codes for re-identifying purposes to permit follow-up of participants will be separately stored in locked premises in the headquarters of the local research partner (to be determined).</p> <p>All data will be entered and downloaded electronically on tablets. These data will be de-identified.</p> <p>Deidentified data will be securely stored on a secure server at UNSW. The electronic files will be stored on a password protected server (Azure, by Microsoft) on a password protected and encrypted platform. On this drive a separate folder for PM+ exists and folders are made for every phase of the study (e.g. formative, pilot, evaluation etc.).</p> <p>All dataset will be pseudonymized and stored on the server, only accessible by primary investigators at UNSW in Sydney.</p>
Archiving and preservation of sensitive data	<p>During the course of STRENGTHS, this list will be stored independently of responses by ensuring all responses are deidentified and linked with names and identifying information in a separate file. The file linking identifying information with unique participant Identification Numbers will be stored at UNSW in locked premises.</p> <p>After completion of STRENGTHS, sensitive data will be stored in electronically on a secure IT network hosted at UNSW accessible. Access will be restricted to research staff directly involved in the study.</p>
Estimated costs of data storage	Data storage will be stored electronically on UNSW server that is provided by UNSW, and therefore there is no cost to STRENGTHS.
Data security	
Use of secure or encrypted communication methods to transfer data	Data will be encrypted using Azure Disk Encryption.
Duration of data storage	Data will be stored for the 7 years following the completion of STRENGTHS.

2.5. Datasets collected in WP5

WP5 Community Implementation	
Data set reference and name	WP5 Community Implementation-The Netherlands
STRENGTHS partner	VUA (Dr. Marit Sijbrandij; e.m.sijbrandij@vu.nl)
Countries where data are gathered	The Netherlands
Purpose of the data collection	To inform the process of comprehensive adaptation of the scalable

	WHO Problem Management Plus (PM+) programmes to reduce psychological distress in Syrian refugees in the Netherlands and to evaluating their effectiveness to reduce psychological distress in Syrian refugees in the Netherlands (WP5)
Type, format and size of data	<p>1. SPSS or Excel data files containing screening data and clinical outcome data from Syrian refugees participating in the STRENGTHS implementation studies in WP5 in the Netherlands. Data files contain information about demographic characteristics (age, education, etc.), symptoms of psychological distress, disability, anxiety, depression, posttraumatic stress-symptoms and health costs. Data will be stored pseudonymous (under participant number, identifying characteristics such as names will be removed). Estimated size: 10 MB</p> <p>2. A list of participant numbers, names and birth dates that matches that SPSS data files under 1. (personal data). Estimated size: 1 MB</p> <p>3. Pen-and-paper surveys of interviews and questionnaires containing screening data and clinical outcome data from Syrian refugees participating in the STRENGTHS implementation studies in WP5 in the Netherlands. Questionnaires contain information about demographic characteristics (age, education, etc.), symptoms of psychological distress, disability, anxiety, depression, posttraumatic stress-symptoms, health service use and health costs. Data will be stored pseudonymous (under participant number, identifying characteristics such as names will be removed).</p> <p>4. Audiotapes (mp3 files) of 100 treatment sessions. Estimated size: 8 GB</p> <p>5. Approx. 1500 paper- and-pencil informed consent forms with name and signature (word documents).</p> <p>6. Qualitative interviews in study participants and key informants after completion of exploratory trial and definitive trial: 1hr per interview (± 300Mb).</p>
Data Sharing	<p>Pseudonymous qualitative transcriptions and datasets described under 6) (see above) will be merged with similar data collected in WP4, 5 and 6. This merged dataset will be shared with LSHTM and KIT in WP2.</p> <p>Pseudonymous quantitative datasets described under 1) will be merged with similar data collected in WP4, 5 and 6 and shared with LSE and VUA for re-use in WP7. In addition, the dataset will be made available upon request for STRENGTHS partners who are interested to answer additional scientific research questions.</p>
Reuse of existing data and origin of existing data	Not applicable
Pseudonymous data to be stored, storing and transfer locations	<p>All data in the data set will be stored pseudonymous, and they will be available only to the VUA research team members.</p> <p>All pseudonymous data to be stored at the VU, will be stored in a data repository named DataverseNL. DataverseNL is an online platform that can be used to share and publish research data in a (semi-) open environment. It is possible to link to a DataverseNL dataset in publications.</p>
Archiving and preservation of sensitive data	Sensitive data to be stored during the course of STRENGTHS are mp3 files of treatment sessions. During the course of STRENGTHS they will be encrypted and stored on in a folder on Surfdrive (a secure cloud

	<p>service for the Dutch education and research community), that can only be accessed by the members of the VUA research team. After the completion of STRENGTHS, the mp3 files will be destroyed.</p> <p>In addition, a list of participant names and participant numbers will be stored. During the course of STRENGTHS, this list will be stored on in a folder Surfdrive that can only be accessed by the members of the VUA research team.</p> <p>After completion of STRENGTHS, it will be stored in DarkStor, an offline research data archive for sensitive data. Data in DarkStor are only accessible by authorized persons (principal investigator).</p>
Estimated costs of data storage	<p>There are no costs involved in data management during the course of STRENGTHS since there is sufficient capacity for data storage on VUA's Surfdrive cloud service.</p> <p>VUA provides 50GB for long-term storage in DataverseNL without costs, which will be sufficient. Archiving in DarkStor costs 2 per GB, therefore we expect to pay euro 30 for archiving in DarkStor for a period of 15 years.</p>
Data security	
Use of secure or encrypted communication methods to transfer data	Data will be encrypted using the encryption software that is used in Surfdrive. Files that are shared with other partners will be sent through Surfdrive.
Duration of data storage	15 years after completion of STRENGTHS (January 2022).

Data set reference and name	WP5 Community Implementation-Turkey
STRENGTHS partner	ISU (Dr. Ceren Acarturk, cerenacarturk@sehir.edu.tr)
Countries where data are gathered	Turkey
Purpose of the data collection	To inform the process of comprehensive adaptation of the scalable WHO Problem Management Plus (PM+) programmes to reduce psychological distress in Syrian refugees in Turkey and to evaluating their effectiveness to reduce psychological distress in Syrian refugees in Turkey (WP5)
Type, format and size of data	<ol style="list-style-type: none"> 1. SPSS or Excel data files containing screening data and clinical outcome data from Syrian refugees participating in the STRENGTHS implementation studies in WP5 in Turkey. Data files contain information about demographic characteristics (age, education, etc.), symptoms of psychological distress, disability, anxiety, depression, posttraumatic stress-symptoms and health costs. Data will be stored pseudonymous (under participant number, identifying characteristics such as names will be removed). Estimated size: 10 MB 2. A list of participant numbers, names and birth dates that matches that SPSS data files under 1. (personal data). Estimated size: 1 MB 3. Pen-and-paper surveys of interviews and questionnaires containing screening data and clinical outcome data from Syrian refugees participating in the STRENGTHS implementation studies in WP5 in Turkey. Questionnaires contain information about demographic characteristics (age, education, etc.), symptoms of psychological distress, disability, anxiety, depression, posttraumatic stress-symptoms, health service use and health costs. Data will be stored pseudonymous

	<p>(under participant number, identifying characteristics such as names will be removed).</p> <p>4. Approx. 1500 paper- and-pencil informed consent forms with name and signature (word documents).</p> <p>5. Qualitative interviews in study participants and key informants after completion of exploratory trial and definitive trials: 1hr per interview (\pm300Mb).</p>
Data Sharing	<p>Pseudonymous qualitative transcriptions and datasets described under 5) (see above) will be merged with similar data collected in WP4, 5 and 6. This merged dataset will be shared with LSHTM and KIT in WP2.</p> <p>Pseudonymous quantitative datasets described under 1) will be merged with similar data collected in WP4, 5 and 6 and shared with LSE and VUA for re-use in WP7. In addition, the dataset will be made available upon request for STRENGTHS partners who are interested to answer additional scientific research questions.</p>
Reuse of existing data and origin of existing data	Not applicable
Pseudonymous data to be stored, storing and transfer locations	<p>All data in the data set will be stored pseudonymous, and they will be available only to the ŞEHİR research team members.</p> <p>All pseudonymous data to be stored at ŞEHİR, will be stored in a data repository named ŞEHİR Academic Repository (DSpace) is an online platform that can be used to share and publish research data in a (semi-) open environment. It is possible to link to a ŞEHİR Academic Repository (DSpace) dataset in publications.</p>
Archiving and preservation of sensitive data	<p>Sensitive data to be stored during the course of STRENGTHS are word documents of treatment sessions. During the course of STRENGTHS they will be encrypted and stored on in a folder on the Home or Group directories of the ŞEHİR network that can only be accessed by the members of the ŞEHİR research team. After the completion of STRENGTHS, they will be destroyed.</p> <p>In addition, a list of participant names and participant numbers will be stored. During the course of STRENGTHS, this list will be stored on in a folder on the ŞEHİR-directory of the ŞEHİR network that can only be accessed by the members of the ŞEHİR research team.</p> <p>After completion of STRENGTHS, it will be stored in ŞEHİR PSYCHOLOGY LAB Archive as encrypted using VeraCrypt software in a CD. Archive is only accessible by authorized persons.</p>
Estimated costs of data storage	<p>There are no costs involved in data management during the course of STRENGTHS since there is sufficient capacity for data storage on the Home and Group directories of ŞEHİR.</p> <p>ŞEHİR provides 50GB for long-term storage in ŞEHİR Academic Repository (DSpace) without costs, which will be sufficient.</p>
Data security	
Use of secure or encrypted communication methods to transfer data	Data will be encrypted using VeraCrypt software.
Duration of data storage	5 years after balance payment of STRENGTHS (2027).

Data set reference and name	WP5 Community Implementation-Switzerland
STRENGTHS partner	UZH (Dr. Naser Morina; naser.morina@usz.ch)
Countries where data are gathered	Switzerland
Purpose of the data collection	To inform the process of comprehensive adaptation of the scalable WHO Problem Management Plus (PM+) programmes to reduce psychological distress in Syrian refugees in Switzerland and to evaluating their effectiveness to reduce psychological distress in Syrian refugees in Switzerland (WP5)
Type, format and size of data	<ol style="list-style-type: none"> 1. SPSS or Excel data files containing screening data and clinical outcome data from Syrian refugees participating in the STRENGTHS implementation studies in WP5 in Switzerland. Data files contain information about demographic characteristics (age, education, etc.), symptoms of psychological distress, disability, anxiety, depression, posttraumatic stress-symptoms, health service use and health costs. Data will be stored pseudonymous (under participant number, identifying characteristics such as names will be removed). Estimated size: 10 MB 2. A list of participant numbers, names and birth dates that matches that SPSS data files under 1. (personal data). Estimated size: 1 MB 3. Surveys of interviews and questionnaires containing screening data and clinical outcome data from Syrian refugees participating in the STRENGTHS implementation studies in Switzerland will be collected on electronic tablets and data automatically downloaded. Questionnaires contain information about demographic characteristics (age, education, etc.), symptoms of psychological distress, disability, anxiety, depression, posttraumatic stress-symptoms, health service use and health costs. Data will be stored pseudonymous (under participant number, identifying characteristics such as names will be removed). 4. Audiotapes (mp3 files) of 100 treatment sessions. Estimated size: 8 GB 5. Approx. 2000 paper- and-pencil informed consent forms with name and signature (word documents). 6. Qualitative interviews in study participants and key informants after completion of exploratory trial and definitive trials: 1hr per interview (± 300Mb).
Data Sharing	<p>Pseudonymous quantitative datasets described under 1) will be merged with similar data collected in WP4, 5 and 6 and shared with LSE and VUA for re-use in WP7. In addition, the dataset will be made available upon request for STRENGTHS partners who are interested to answer additional scientific research questions.</p> <p>Pseudonymous qualitative transcriptions and datasets described under 6) (see above) will be merged with similar data collected in WP4, 5 and 6. This merged dataset will be shared with LSHTM and KIT in WP2.</p>
Reuse of existing data and origin of existing data	Not applicable
Pseudonymous data to be stored, storing and transfer locations	<p>All data in the data set will be stored pseudonymous, and they will be available only to the UZH research team members.</p> <p>All anonymous pseudonymous data to be stored at UZH, will be stored on a secure server at University Hospital Zurich.</p>

Archiving and preservation of sensitive data	<p>Sensitive data to be stored during the course of STRENGTHS are mp3 files of treatment sessions. During the course of STRENGTHS they will be encrypted and stored in the research server of the University Hospital Zurich network that can only be accessed by member of the UZH research team. After the completion of the STRENGTHS project, they will be destroyed.</p> <p>In addition, a list of participant names and participant code will be stored. During the course of STRENGTHS, this list will be stored on in a folder on the research server of the UZH network that can only be accessed by the members of the UZH research team.</p>
Estimated costs of data storage	There are no costs involved in data management during the course of STRENGTHS since there is sufficient capacity for data storage on the home and research servers of UZH.
Data security	
Use of secure or encrypted communication methods to transfer data	Data will be transferred via a secured We Transfer Account or an FTP server. Data will be encrypted using VeraCrypt software.
Duration of data storage	10 years after completion of STRENGTHS (January 2022)

2.6. Datasets collected in WP6

WP6 Online Implementation	
Data set reference and name	WP6 Online Implementation
STRENGTHS partner	FUB (Prof. Christine Knaevelsrud; christine.knaevelsrud@fu-berlin.de)
Countries where data are gathered	Germany, Sweden, Egypt
Purpose of the data collection	<p>Development and scientific evaluation of a smartphone and internet based psychological intervention for Syrian refugees with common mental health problems. This results in two main purposes for data collection:</p> <ol style="list-style-type: none"> 1. Making informed decisions on how to design and implement the intervention. 2. Assessing health outcomes of the intervention.
Type, format and size of data	<ol style="list-style-type: none"> 1. SPSS or Excel data files containing screening data and clinical outcome data and app usage statistics in CSV file format from Syrian refugees participating in the STRENGTHS implementation studies in WP6 in Germany, Sweden and Egypt. Data files contain information about demographic characteristics (age, education, etc.), symptoms of psychological distress, disability, anxiety, depression, posttraumatic stress-symptoms, health service use and health costs. Data will be stored pseudonymous (under participant number, identifying characteristics such as names will be removed). Estimated size: 1 GB 2. A list of participant numbers, names and birth dates that matches that SPSS data files under 1. (personal data). Estimated size: 1 MB 3. Approx. 80 paper- and-pencil informed consent forms with name and signature (word documents). 4. Qualitative interviews in study participants and key informants after

	completion of exploratory trial and definitive trials: 1hr per interview ($\pm 300\text{Mb}$).
Data Sharing	Pseudonymous quantitative datasets described under 1) will be merged with similar data collected in WP4, 5 and 6 and shared with LSE and VUA for re-use in WP7. In addition, the dataset will be made available upon request for STRENGTHS partners who are interested to answer additional scientific research questions.
Reuse of existing data and origin of existing data	Not applicable
Pseudonymous data to be stored, storing and transfer locations	The app transfers the data regularly from the users' device to a database on a secure server where it is stored with a unique API token (or ID) that is bound to a users' app installation. Pseudonymous data will be transferred to workstations at FUB for statistical data analysis. All pseudonymous data to be stored at FUB, will be stored in the FUB institutional data repository (currently unnamed). The repository is currently in the last phase of development and will be ready for use in autumn 2017.
Archiving and preservation of sensitive data	For qualitative interviews and focus group discussions the following sensitive data (= data that allows conclusions about who the persons involved in the study are) will be assessed: <ul style="list-style-type: none"> – name and contact information (phone or email) – age and gender – place and date of the interview/discussion – group (e.g. scientific expert, refugee, helper) Name and contact information of all participants in the qualitative interviews and focus groups appear only on the informed consent paper forms that will be stored separately from all other data in a locked file cabinet at FUB. Users of the app will provide: <ul style="list-style-type: none"> – user name (not their real name) – contact information (mobile number or email) – age, gender and level of education The researchers that conduct the interviews and focus groups will transfer the sensitive data from the different locations of the interviews/discussion (in Sweden, Germany and Egypt) to FUB. The app will transfer sensitive data to a separate database (not the one used for pseudonymous data described below). This separate system is part of the contact-on-demand backend of the intervention and is located on a secure server.
Estimated costs of data storage	no costs
Data security	
Use of secure or encrypted communication methods to transfer data	TLS encryption protects all data transferred from and to the app.
Duration of data storage	10 years

2.7. Datasets collected in WP7

WP7 Economic and Implementation Evaluation	
Data set reference and name	
STRENGTHS partner	LSE (David McDaid; D.McDaid@lse.ac.uk) and VUA (Marit Sijbrandij)
Countries where data are gathered	All project countries. Note: WP7 will not generate data sets other than information from project partners on their own activities for facilitating implementation, but partners in WP7 (LSE and VUA) will perform secondary data analysis on pseudonymous data collected in WP2, WP4, 5 and 6.
Purpose of the data collection	To estimate economic costs of implementing the scalable WHO psychological programs To determine cost-effectiveness of the scalable WHO psychological programs across project countries. To model interactions between the effectiveness of the scalable WHO psychological programs and refugee and context characteristics.
Type, format and size of data	Pseudonymised SPSS dataset, expected size: 100 MB. SPSS dataset summarising resources and time invested by partners in implementation activities.
Data Sharing	No data will be shared by partners in WP7
Reuse of existing data and origin of existing data	WP7 will use existing data to perform secondary data analysis on pseudonymous data collected in WP2, WP4, 5 and 6.
Pseudonymous data to be stored, storing and transfer locations	LSE: All data shared with the LSE will be securely stored on the LSE server, and only accessible to the LSE STRENGTHS team. VUA: during the course of STRENGTHS, data will be stored on Surfdrive (a secure cloud service for the Dutch education and research community), that can only be accessed by the members of the VUA research team. After completion of STRENGTHS, data will be stored in DarkStor, an offline research data archive for sensitive data. Data in DarkStor are only accessible by authorized persons (principal investigator).
Archiving and preservation of sensitive data	No sensitive data will be archived in WP7.
Estimated costs of data storage	No costs are involved, since both LSE and VUA have sufficient space on the servers to store the data.
Data security	
Use of secure or encrypted communication methods to transfer data	In WP7, no data will be transferred.
Duration of data storage	LSE: 5 years VUA: 15 years


2.8. Datasets collected in WP8

WP8 Dissemination and synthesis	
Data set reference and name	WP8 website and newsletter data
STRENGTHS partner	DRC (Louise Juul Hansen)
Countries where data are gathered	Potentially all countries globally, more likely countries in EU and the MENA region with a preponderance of STRENGTHS project countries.
Purpose of the data collection	<p>A: Monitoring traffic on the project website, www.strengths-project.eu The purpose of monitoring traffic on the website is to be able to measure the number of users, to identify possible problems on the page or opportunities for improvement. It is also hoped that information about the geographical distribution of website users may help identify opportunities for further dissemination.</p> <p>B: To improve segmentation of newsletters data from persons who sign up to the newsletter will be collected on a voluntary basis. Readers are bound to share their email to receive the newsletter, but additional information such as organization, title, country of residence, country of origin will be collected on a strictly voluntary basis.</p>
Type, format and size of data	<p>A: Anonymized data on traffic on the website, e.g. how many visits to a page, how long the user stays on a page, in which country the user's IP address is located, which type of device the user uses etc. Service used to collect and store data: Google Analytics</p> <p>B: Information about subscriber's email address (obligatory) and country, organization, position (voluntary). Service used to collect and store data: MailChimp.</p>
Data Sharing	No data will be shared by partners in WP8
Reuse of existing data and origin of existing data	No reuse is foreseen
Pseudonymous data to be stored, storing and transfer locations	N/A
Archiving and preservation of sensitive data	No sensitive data will be archived in WP8.
Estimated costs of data storage	No costs are involved.
Data security	
Use of secure or encrypted communication methods to transfer data	In WP8, no data will be transferred.
Duration of data storage	No longer than till project closure, 31/12/2021


3. STRENGTHS partners involved in STRENGTHS Data Management


The tables below provide an overview of all STRENGTHS partners that are involved in collecting, storing or otherwise handling STRENGTHS research data. They provide details concerning individuals in their institutions involved in data management, and local and national regulations and procedures in place concerning data management.

STRENGTHS partner	VUA (VU University Amsterdam) 
Principal Investigator responsible for data management	Dr. Marit Sijbrandij (e.m.sijbrandij@vu.nl)
Data Protection Officer within institution	Mr. Petra Tolen
Information Security Officer within institution	Drs. Nicole van Deursen
Applicable national/funder/sectorial/departmental procedures for data management	<p>1. Medical Research Involving Human Subjects Act [Wet op Medisch-Wetenschappelijk Onderzoek; WMO; see http://www.ccmo.nl/en/]</p> <p>2. Dutch Personal Data Protection Act [Wet op de Bescherming van de Persoonsgegevens; see: https://www.akd.nl/en/a/Pages/English-translation-of-the-Dutch-Personal-Data-Protection-Act---Wet-Bescherming-Persoonsgegevens-(WBP)-in-English.aspx] and the Code of Conduct of Health Research based on the Dutch Personal Data Protection Act. VUA will submit the VUA STRENGTHS studies at the Dutch Authority Personal Data Protection [Autoriteit Persoonsgegevens].</p> <p>3. VU University has a Standard Evaluation Protocol (SEP) to handle research data (see https://www.vu.nl/nl/Images/Protocol_Onderzoeksevaluatie_vastgesteld_tcm289-413353.pdf). This protocol meets the regulations specified in the Dutch Personal Data Protection Act.</p>
Ethics	All studies carried out by VU University will be submitted for review to the Medical Ethics Review Committee (METc) of the VU Medical Center (see https://www.vumc.nl/afdelingen/METc/).


STRENGTHS partner	DRC (Reference Center for Psychosocial Support hosted by Danish Red Cross) 
Principal Investigator responsible for data management	Martha Bird (mabir@rodekors.dk)
Data Protection Officer within institution	Mr Brigitte Bischoff Ebbesen and Mr Lars Mejlbohm
Information Security Officer within institution	Mr Arne Cæsar Bisgaard Christiansen
Applicable national/	Guidance on procedures from the Danish Data Protection Agency is


funder/sectorial/departme ntal procedures for data management	followed in the design of the procedures for DRC. As a precautionary measure, the tests are reported to the same agency as well as to the Danish National Committee on Health Research Ethics according to their templates.
Ethics	Studies carried out by DRC that need ethics review, will be submitted for review to De Videnskabetiske komiteer, Region Hovedstaden” (https://www.regionh.dk/vek).


STRENGTHS partner	FUB (Freie Universität Berlin)  Freie Universität Berlin
Principal Investigator responsible for data management	Prof. Dr. Christine Knaevelsrud (christine.knaevelsrud@fu-berlin.de)
Data Protection Officer within institution	Mrs. Ingrid Pahlen-Brandt
Information Security Officer within institution	Mr. Dietmar Dräger
Applicable national/ funder/sectorial/departme ntal procedures for data management	FUB has no published document on data management procedures but there is a Research Data Management Official (Mrs. Petra Buchholz). We will use the procedures suggested by Mrs. Buchholz and we will follow the “Proposals for Safeguarding Good Scientific Practice” by the German Research Foundation (DFG). In regard to data security, FUB will comply with the following regulations: 1. Berlin Data Security Act (Berliner Datenschutzgesetz in German) 2. Federal Data Protection Act (<i>Bundesdatenschutzgesetz</i> in German) (BDSG) 3. FUB guidelines for IT Security (IT-Sicherheitsrichtlinie in German) 4. EU General Data Protection Regulation (GDPR)
Ethics	Studies carried out by FUB will be submitted for review to Freie Universität Research Ethics Committee


STRENGTHS partner	IMC (International Medical Corps)  International Medical Corps
Principal Investigator responsible for data management	Claire Whitney (cwhitney@InternationalMedicalCorps.org)
Data Protection Officer within institution	Emebet Dlasso Menna
Information Security Officer within institution	Yazan Smadi
Applicable national/ funder/sectorial/departme ntal procedures for data management	Within the mandate of IMC’s Monitoring & Evaluation minimum quality standards, data management and confidentiality are followed to maintain relevant personal data according to the General Data Protection Regulation (EU) 2016/679..


Ethics	IMC will not need to apply for ethics approval for studies to be carried out in WP3.
---------------	--

STRENGTHS partner	IPSY (i-Psy Midden en Noord Nederland)
Principal Investigator responsible for data management	Yvette van Son (Y.vanSon@i-psy.nl) 
Data Protection Officer within institution	Gert-Jan Tupker
Information Security Officer within institution	Frans Jansen
Applicable national/funder/sectorial/departementaal procedures for data management	1. Medical Research Involving Human Subjects Act [Wet op Medisch-Wetenschappelijk Onderzoek; WMO; see http://www.ccmo.nl/en/] 2. Dutch Personal Data Protection Act [Wet op de Bescherming van de Persoonsgegevens; see: https://www.akd.nl/en/a/Pages/English-translation-of-the-Dutch-Personal-Data-Protection-Act---Wet-Bescherming-Persoonsgegevens-(WBP)-in-English.aspx] and the Code of Conduct of Health Research based on the Dutch Personal Data Protection Act.
Ethics	Studies in which i-Psy is involved, will be submitted for review by VUA to the Medical Ethics Review Committee (METc) of the VU Medical Center.

STRENGTHS partner	KIT (KIT Royal Tropical Institute) 
Principal Investigator responsible for data management	Dr. Egbert Sondorp (e.sondorp@kit.nl)
Data Protection Officer within institution	Louis van den Berghe
Information Security Officer within institution	Maurice van der Hoff
Applicable national/funder/sectorial/departementaal procedures for data management	1. Medical Research Involving Human Subjects Act [Wet op Medisch-Wetenschappelijk Onderzoek; WMO; see http://www.ccmo.nl/en/] 2. Dutch Personal Data Protection Act [Wet op de Bescherming van de Persoonsgegevens; see: https://www.akd.nl/en/a/Pages/English-translation-of-the-Dutch-Personal-Data-Protection-Act---Wet-Bescherming-Persoonsgegevens-(WBP)-in-English.aspx] and the Code of Conduct of Health Research based on the Dutch Personal Data Protection Act. We will also be following our institutional procedures for data management
Ethics	Studies by KIT will be carried out jointly with LSHTM and will be submitted for review by the Ethics Committee of LSHTM and the university partners and national IRBs (where required) in which the work is being conducted. If need be, studies can also be submitted for review by the KIT Ethical Board.


STRENGTHS partner	LSE (London School of Economics and Political Science)	
Principal Investigator responsible for data management	ProfDavid McDaid (d.mcdaid@lse.ac.uk)	
Data Protection Officer within institution	Rachel Maguire (r.e.maguire@lse.ac.uk)/ Andrew Webb	
Information Security Officer within institution	Jethro Perkins (j.a.perkins@lse.ac.uk)	
Applicable national/funder/sectorial/departmental procedures for data management	<p>1. UK Data Protection Act 1998</p> <p>2. As of 25 May 2018 the General Data Protection Regulation (EU) 2016/679 and any additional data protection laws that might come into effect in the United Kingdom after the UK leaves the EU.</p> <p>2) LSS Data Protection and Research guidelines http://www.lse.ac.uk/intranet/LSEservices/policies/pdfs/school/datProRes.pdf</p>	
Ethics	LSE will not collect primary data (other than from project partners themselves on implementation activities), but will re-use data collected by other partners. Therefore, LSE will not need to apply for ethics approval.	

STRENGTHS partner	LSHTM (London School of Hygiene and Tropical Medicine)	
Principal Investigator responsible for data management	Dr. Bayard Roberts (bayard.roberts@lshtm.ac.uk)	
Data Protection Officer within institution	Lucinda Parr	
Information Security Officer within institution	Marion Rosenberg	
Applicable national/funder/sectorial/departmental procedures for data management	<p>1. UK Data Protection Act 1998</p> <p>2. LSHTM will also be following the institutional procedures for data management</p>	
Ethics	Studies carried out by LSHTM will be submitted for review to the Ethics Committee of LSHTM and the university partners and national IRBs (where required) in which the work is being conducted.	


STRENGTHS partner	WCH (War Child Holland)	
Principal Investigator responsible for data management	Dr. Mark Jordans (mark.jordans@warchild.nl)	


Data Protection Officer within institution	Frederik Steen
Information Security Officer within institution	Robin Groeneweg
Applicable national/funder/sectorial/departmenal procedures for data management	<p>1. Medical Research Involving Human Subjects Act [Wet op Medisch-Wetenschappelijk Onderzoek; WMO; see http://www.ccmo.nl/en/]</p> <p>2. Dutch Personal Data Protection Act [Wet op de Bescherming van de Persoonsgegevens; see: https://www.akd.nl/en/a/Pages/English-translation-of-the-Dutch-Personal-Data-Protection-Act---Wet-Bescherming-Persoonsgegevens-(WBP)-in-English.aspx] and the Code of Conduct of Health Research based on the Dutch Personal Data Protection Act. VUA will submit the VUA STRENGTHS studies at the Dutch Authority Personal Data Protection [Autoriteit Persoonsgegevens].</p> <p>3. We are using the Data Management Plan of the Research & Development Department of War Child Holland</p>
Ethics	Studies carried out by WCH will be submitted for review to St. Joseph University, Beirut, Lebanon (https://www.usj.edu.lb/).

STRENGTHS partner	ISU (Istanbul Sehir University)	
Principal Investigator responsible for data management	Dr. Ceren Acarturk (cerenacarturk@sehir.edu.tr)	
Data Protection Officer within institution	Peyami Çelikcan	
Information Security Officer within institution	Cengiz Benli	
Applicable national/funder/sectorial/departmenal procedures for data management	The Turkish Data Protection Law No. 6698 ('DP Law')	
Ethics	Studies carried out by ISU will be submitted for review to the as İstanbul Şehir University Research Ethics Committee.	

STRENGTHS partner	Multeciler Ve Siginmacilar Yardimlasma Ve Day Anisma Dernegi (RASASA)	
Principal Investigator responsible for data management	Mehmet Aktas	
Data Protection Officer within institution	Zafer Sögütçü/ Dernek Başkanı	
Information Security Officer within institution	Ahmet Selman Özdemir	
Applicable national/funder/sectorial/departmenal procedures for data management	The Turkish Data Protection Law No. 6698 ('DP Law')	

funder/sectorial/departme ntal procedures for data management	
Ethics	Studies in which RASASA is involved will be submitted for review by ISU to the as İstanbul Şehir University Research Ethics Committee.

STRENGTHS partner	UNSW (University of New South Wales)	
Principal Investigator responsible for data management	Prof. Richard Bryant (r.bryant@unsw.edu.au)	
Data Protection Officer within institution	Kate Carruthers	
Information Security Officer within institution	Alex Blagus	
Applicable national/ funder/sectorial/departme ntal procedures for data management	<ol style="list-style-type: none"> 1. Privacy and Personal Information Protection Act 1998 (New South Wales) 2. UNSW Data Handling Guidelines 	
Ethics	Studies carried out by UNSW will be submitted for review to the UNSW Psychology Human Research Ethics Approval Panel and UNSW Human Research Ethics Committee.	

STRENGTHS partner	UZH (Universität Zürich)	
Principal Investigator responsible for data management	Dr. Naser Morina (Naser.Morina@usz.ch)	
Data Protection Officer within institution	Dr. iur. Robert Weniger, UZH	
Information Security Officer within institution	Tatyana Rodelli, Franziska Oser-Hefti (University Hospital Zurich)	
Applicable national/ funder/sectorial/departme ntal procedures for data management	<ol style="list-style-type: none"> 1. The Swiss Federal Act of 19 June 1992 on Data Protection (FADP) and the Ordinance of 14 June 1993 to the Swiss Federal Act on Data Protection (OFADP) 2. Data protection guidelines of the University of Zurich and data protection guidelines of the Clinical Trial Centre (University Hospital Zurich). 	
Ethics	Studies carried out by UZH will be submitted for ethics review to the ethics review board of the Canton of Zurich.	

Appendix: Data Protection Labels

Note:

The appendix includes the signed Data Protection labels of all partners collecting and processing data in relation to the EU H2020 STRENGTHS project (733337).

The Data Protection labels are also submitted separately as D9.6.

DATA PROTECTION LABEL VU

Stichting VU, a foundation incorporated under the laws of the Netherlands, maintaining the *Vrije Universiteit Amsterdam* as a privately run university in accordance with the Higher Education and Research Act of The Netherlands (*Wet op het hoger onderwijs en wetenschappelijk onderzoek*), having its registered office and principal place of business in Amsterdam at De Boelelaan 1105, 1081 HV Amsterdam (hereinafter: the: "**Controller**") hereby warrants as follows:

1. Subject matter of this Data Protection Label

- 1.1. This Data Protection Label applies exclusively to the processing of personal data in the scope of the EU H2020 STRENGTHS project.
- 1.2. Terms such as "processing", "personal data", "controller" shall have the meaning ascribed to them in the General Data Protection Regulation (EU) 2016/679 (hereinafter: the "**GDPR**").

2. The processing of personal data

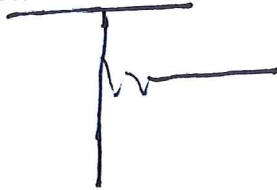
- 2.1. The Controller warrants that it will process the personal data in accordance with the Dutch Data Protection Act (*Wet bescherming persoonsgegevens*) and as of 25 May 2018 in accordance with the GDPR and any additional data protection laws which will come into effect in the Netherlands.
- 2.2. The Controller warrants that it will process the personal data only in such a manner as - and to the extent that - this is necessary for the purposes of the EU H2020 STRENGTHS project.
- 2.3. The personal data will not be processed for other purposes.
- 2.4. The Controller warrants that it shall treat all personal data strictly confidential and that it shall inform all its employees and/or approved (sub-)processors engaged in the processing of personal data of the confidential nature of such information and of the personal data. The Controller shall ensure that all employees or other persons working with the personal data are bound to adequate confidentiality agreements.

3. Security

- 3.1. The Controller warrants that it shall implement appropriate technical, physical and organizational measures to ensure the security of the personal data. These measures shall include in any case:
 - (a) measures to ensure that the personal data can be accessed only by authorized personnel for the purposes of EU H2020 STRENGTHS project.
 - (b) measures to protect the personal data against accidental or unlawful destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure;
 - (c) measures to identify vulnerabilities with regard to the processing of personal data in systems used by the Controller.
- 3.2. The Controller shall at all times have in place a suitable, written security policy with respect to the processing of personal data, outlining in any case the measures set forth in 3.1.

3.3. The Controller acknowledges that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures.

Signature:



Name:

Tom Paffen

Title:

Privacy Officer

Date signed:

7 June 2017

DATA PROTECTION LABEL DRC

Danish Red Cross (hereinafter DRC), incorporated under the laws of Denmark, having its registered office and principal place of business at Blegdamsvej 27, 2100 Copenhagen, Denmark hereby warrants as follows:

1. Subject matter of this Data Protection Label

- 1.1. This Data Protection Label applies exclusively to the processing of personal data in the scope of the STRENGTHS project, grant number 733337 funded under the H2020 Framework.
- 1.2. Terms such as "processing", "personal data", "data controller" shall have the meaning ascribed to them in the Danish Data Protection Act (*Persondataloven (lov nr 439 af 31. Maj 2000)*).

2. The processing of personal data

- 2.1. DRC warrants that it will process the personal data only in such a manner as - and to the extent that - this is necessary for the purposes of STRENGTHS project, as defined in the Description of Work of grant number 733337. The personal data will not be processed for other purposes.
- 2.2. DRC warrants that it shall treat all personal data strictly confidential and that it shall inform all its employees and/or approved (sub-)processors engaged in the processing of personal data as part of the STRENGTHS project of the confidential nature of such information and of the personal data. DRC ensures that all employees or other persons working with the personal data of the STRENGTHS project are bound to adequate confidentiality agreements.

3. Security

- 3.1. DRC warrants that it shall implement appropriate technical, physical and organizational measures to ensure the security of the personal data. These measures shall include in any case:
 - (a) measures to ensure that the personal data can be accessed only by authorized personnel for the purposes of STRENGTHS;
 - (b) measures to protect the personal data against accidental or unlawful destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure;
 - (c) measures to identify vulnerabilities with regard to the processing of personal data in systems used by the data controller.
- 3.2. For the STRENGTHS project the following measures are in place with respect to the processing of personal data, outlining in any case the measures set forth in 3.1:
 - 3.2.1. The DRC secure server. Data is stored only on the server and only in specific, password protected files only available to the staff working on STRENGTHS and the signatories to this document, as stated below
 - 3.2.2. Safe and stable VPN access to the DRC servers so data can be accessed at any time, thereby eliminating the need for storing data locally on laptops or flash drives



DANISH
RED
CROSS

- 3.2.3. The DRC email (@rodekors.dk) is safeguarded through encryption allowing DRC staff to correspond on and share data files securely across locations
 - 3.2.4. The DRC "secure email" setup, which encrypts the email and data that is being transferred and establishes a secure channel of communication between @rodekors.dk emails and other mailbox systems. This setup allows STRENGTHS project partners to transfer data secure to and from DRC.
 - 3.2.5. Personal laptops are password protected, and run Window10 with Bitlocker device encryption
- 3.3. DRC acknowledges that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures.

4. Signatures

Name: Lars Meibom
Title: Head of Shared Services
Date signed: 15/6-2017

Name: Birgitte Bishoff Ebbesen
Title: Head of International Dept.
Date signed: 08/06/2017

DATA PROTECTION LABEL Freie Universität Berlin

Freie Universität Berlin, a public research institution under the laws of Germany, having its registered office and principal place of business in Kaiserswerther Str. 16-18, 14195 Berlin, Germany, on behalf of its Division of Clinical Psychologic Intervention, PI: Prof. Dr. Christine Knaevelsrud, FUB Contract Nr. 2017000154 (hereinafter: the: "**Controller**") hereby warrants as follows:

1. Subject matter of this Data Protection Label

- 1.1. This Data Protection Label applies exclusively to the processing of personal data in the scope of the EU H2020 STRENGTHS project.
- 1.2. Terms such as "processing", "personal data", "controller" shall have the meaning ascribed to them in the General Data Protection Regulation (EU) 2016/679 (hereinafter: the "**GDPR**").

2. The processing of personal data

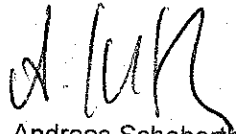
- 2.1. The Controller warrants that it will process the personal data in accordance with the German Data Protection Act (Bundesdatenschutzgesetz; BDSG) and the Berlin Data Protection Act (Berliner Datenschutzgesetz, BlnDSG) and as of 25 May 2018 in accordance with the GDPR and any additional data protection laws which will come into effect in Germany.
- 2.2. The Controller warrants that it will process the personal data only in such a manner as - and to the extent that - this is necessary for the purposes of the EU H2020 STRENGTHS project.
- 2.3. The personal data will not be processed for other purposes.
- 2.4. The Controller warrants that it shall treat all personal data strictly confidential and that it shall inform all its employees and/or approved (sub-)processors engaged in the processing of personal data of the confidential nature of such information and of the personal data. The Controller shall ensure that all employees or other persons working with the personal data are bound to adequate confidentiality agreements.

3. Security

- 3.1. The Controller warrants that it shall implement appropriate technical, physical and organizational measures to ensure the security of the personal data. These measures shall include in any case:
 - (a) measures to ensure that the personal data can be accessed only by authorized personnel for the purposes of EU H2020 STRENGTHS project.
 - (b) measures to protect the personal data against accidental or unlawful destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure;
 - (c) measures to identify vulnerabilities with regard to the processing of personal data in systems used by the Controller.
- 3.2. The Controller shall at all times have in place a suitable, written security policy with respect to the processing of personal data, outlining in any case the measures set forth in 3.1.

3.3. The Controller acknowledges that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures.

Signature



Name

Dr. Andreas Schoberth

Title

Head of Legal Affairs in Research & Transfer

Date signed

16.06.2017

DATA PROTECTION LABEL IMC UK

The International Medical Corps UK, a Charity incorporated under the laws of England and Wales, having its registered office and principal place of business in London at 161 Marsh Wall, E14 9SJ, United Kingdom (hereinafter to be referred to as the 'Controller') hereby warrants as follows:

1. Subject matter of this Data Protection Label

- 1.1. This Data Protection Label applies exclusively to the processing of personal data in the scope of the EU H2020 STRENGTHS (Syrian REfuGees MeNTal Health Care Systems) project.
- 1.2. Terms such as "processing", "personal data", "data controller" shall have the meaning ascribed to them in the General Data Protection Regulation (EU) 2016/679 (hereinafter: the "GDPR").

2. The processing of personal data

- 2.1. The Controller warrants that it will process the personal data in accordance with the EU Data Protection Act 1998 (hereinafter: the 'Act') and as of 25 May 2018 in accordance with the GDPR and any additional data protection laws which will come into effect in the United Kingdom.
- 2.2. The Controller warrants that it will process the personal data only in such a manner as – and to the extent that – this is necessary for the purposes of the EU H2020 STRENGTHS project.
- 2.3. The personal data will not be processed for other purposes
- 2.4. The Controller warrants that it shall treat all personal data strictly confidential and that it shall inform all its employees and/or approved (sub)processors engaged in the processing of personal data of the confidential nature of such information and of the personal data. The Controller shall ensure that all employees or other persons working with the personal data are bound to adequate confidentiality agreements.

3. Security

- 3.1. The Data Controller warrants that it shall implement appropriate technical, physical and organizational measures to ensure the security of the personal data. These measures shall include in any case:
 - (a) measures to ensure that the personal data can be accessed only by authorized personnel for the purposes of STRENGTHS;

Board of Trustees

Andrew W. Géczy
(Chairman)

Nancy A. Aossey

Timothy S. Kirk

C. William Sundblad





161 Marsh Wall, London, E14 9SJ
Tel: +44 (0)20 7253 0001
Web: www.internationalmedicalcorps.org.uk
Email: info@internationalmedicalcorps.org.uk

(b) measures to protect the personal data against accidental or unlawful destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure;

(c) measures to identify vulnerabilities with regard to the processing of personal data in systems used by the data controller.

3.2. The Controller shall at all times have in place a suitable, written security policy with respect to the processing of personal data, outlining in any case the measures set forth in 3.1.

3.3. The Data Controller acknowledges that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures.

Signature:

A handwritten signature in black ink, appearing to read 'EMEBET D. MENNA', written over a horizontal line.

Name: Emebet Dlasso Menna

Title: Grants and MEAL Coordinator

Date signed: June 11, 2017

Board of Trustees

Andrew W. Géczy
(Chairman)

Nancy A. Aosse

Timothy S. Kirk

C. William Sundblad

DATA PROTECTION LABEL i-psy

i-psy Midden en Noord Nederland, a foundation incorporated under the laws of the Netherlands, having its registered office and principal place of business in Almere at Metropolestraat 1C, 1315 KK Almere (hereinafter: the "**Controller**") hereby warrants as follows:

1. Subject matter of this Data Protection Label

- 1.1. This Data Protection Label applies exclusively to the processing of personal data in the scope of the EU H2020 STRENGTHS project.
- 1.2. Terms such as "processing", "personal data", "controller" shall have the meaning ascribed to them in the General Data Protection Regulation (EU) 2016/679 (hereinafter: the "**GDPR**").

2. The processing of personal data

- 2.1. The Controller warrants that it will process the personal data in accordance with the Dutch Data Protection Act (*Wet bescherming persoonsgegevens*, hereinafter: the "**Wbp**") and as of 25 May 2018 in accordance with the GDPR and any additional data protection laws which will come into effect in the Netherlands.
- 2.2. The Controller warrants that it will process the personal data only in such a manner as - and to the extent that - this is necessary for the purposes of the EU H2020 STRENGTHS project.
- 2.3. The personal data will not be processed for other purposes.
- 2.4. The Controller warrants that it shall treat all personal data strictly confidential and that it shall inform all its employees and/or approved (sub-)processors engaged in the processing of personal data of the confidential nature of such information and of the personal data. The Controller shall ensure that all employees or other persons working with the personal data are bound to adequate confidentiality agreements.

3. Security

- 3.1. The Controller warrants that it shall implement appropriate technical, physical and organizational measures to ensure the security of the personal data. These measures shall include in any case:
 - (a) measures to ensure that the personal data can be accessed only by authorized personnel for the purposes of EU H2020 STRENGTHS project.
 - (b) measures to protect the personal data against accidental or unlawful destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure;
 - (c) measures to identify vulnerabilities with regard to the processing of personal data in systems used by the Controller.
- 3.2. The Controller shall at all times have in place a suitable, written security policy with respect to the processing of personal data, outlining in any case the measures set forth in 3.1.



3.3. The Controller acknowledges that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures.

Signature

Name: Gert-Jan Tupker

Title: Bestuurder

Date signed: 28-06-2017



DATA PROTECTION LABEL KIT (Royal Tropical Institute)

KIT (Royal Tropical Institute), an association incorporated under the laws of the Netherlands, having its registered office and principal place of business in Amsterdam at Mauritskade 63, Amsterdam, the Netherlands (hereinafter to be referred to as: the: "**Data Controller**") hereby warrants as follows:

1. Subject matter of this Data Protection Label

- 1.1. This Data Protection Label applies exclusively to the processing of personal data in the scope of the EU H2020 STRENGTHS project.
- 1.2. Terms such as "processing", "personal data", "data controller" shall have the meaning ascribed to them in the General Data Protection Regulation (EU) 2016/679.

2. The processing of personal data

- 2.1. The Data Controller warrants that it will process the personal data in accordance with the Dutch Data Protection Act (Wet bescherming persoonsgegevens, hereinafter : the "Wbp") and as of 25 May 2018 in accordance with the General Data Protection Regulation (EU) 2016/679 and any additional data protection laws which will come into effect in the Netherlands.
- 2.2. The Data Controller warrants that it will process the personal data only in such a manner as - and to the extent that - this is necessary for the purposes of the EU H2020 STRENGTHS project.
- 2.3. The personal data will not be processed for other purposes.
- 2.4. The Data Controller warrants that it shall treat all personal data strictly confidential and that it shall inform all its employees and/or approved (sub-)processors engaged in the processing of personal data of the confidential nature of such information and of the personal data. The Data Controller shall ensure that all employees or other persons working with the personal data are bound to adequate confidentiality agreements.

3. Security

- 3.1. The Data Controller warrants that it shall implement appropriate technical, physical and organizational measures to ensure the security of the personal data. These measures shall include in any case:
 - (a) measures to ensure that the personal data can be accessed only by authorized personnel for the purposes of the STRENGTHS project;
 - (b) measures to protect the personal data against accidental or unlawful destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure;
 - (c) measures to identify vulnerabilities with regard to the processing of personal data in systems used by the data controller.
- 3.2. The Data Controller shall at all times have in place a suitable, written security policy with respect to the processing of personal data, outlining in any case the measures set forth in 3.1.



3.3. The Data Controller acknowledges that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures.

Signature

Name

L.J. van der Berghe

Title

CFO

Date signed

13/06/2017

DATA PROTECTION LABEL LSE

The London School of Economics, a company limited by guarantee (Register number: 70257) and an exempt charity under the laws of the United Kingdom, having its registered office and principal place of business in Houghton Street, London WC2A 2AE (hereinafter to be referred to as: the "Data Controller") hereby warrants as follows:

1. Subject matter of this Data Protection Label

- 1.1. This Data Protection Label applies exclusively to the processing of personal data in the scope of the EU H2020 STRENGTHS project.
- 1.2. Terms such as "processing", "personal data", "data controller" shall have the meaning ascribed to them in the General Data Protection Regulation (EU) 2016/679.

2. The processing of personal data

- 2.1. The Data Controller warrants that it will process the personal data in accordance with the UK Data Protection Act (DPA) and as of 25 May 2018 in accordance with the General Data Protection Regulation (EU) 2016/679 and any additional data protection laws which will come into effect in the United Kingdom.
- 2.2. The Data Controller warrants that it will process the personal data only in such a manner as - and to the extent that - this is necessary for the purposes of the EU H2020 STRENGTHS project.
- 2.3. The personal data will not be processed for other purposes.
- 2.4. The Data Controller warrants that it shall treat all personal data strictly confidential and that it shall inform all its employees and/or approved (sub-)processors engaged in the processing of personal data of the confidential nature of such information and of the personal data. The Data Controller shall ensure that all employees or other persons working with the personal data are bound to adequate confidentiality agreements.

3. Security

- 3.1. The Data Controller warrants that it shall implement appropriate technical, physical and organizational measures to ensure the security of the personal data. These measures shall include in any case:
 - (a) measures to ensure that the personal data can be accessed only by authorized personnel for the purposes of EU H2020 STRENGTHS project.
 - (b) measures to protect the personal data against accidental or unlawful destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure;
 - (c) measures to identify vulnerabilities with regard to the processing of personal data in systems used by the data controller.

3.2. The Data Controller shall at all times have in place a suitable, written security policy with respect to the processing of personal data, outlining in any case the measures set forth in 3.1.

3.3. The Data Controller acknowledges that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures.

Signature *Andrew Webb*

Name ANDREW WEBB

Title SECRETARY

Date signed 22 June 2017



DATA PROTECTION LABEL LSHTM

The London School of Hygiene and Tropical Medicine (hereinafter to be referred to as the “Data Controller”) hereby warrants as follows:

1. Subject matter of this Data Protection Label

- 1.1. This Data Protection Label applies exclusively to the processing of personal data in the scope of the EU H2020 STRENGTHS project.
- 1.2. Terms such as “processing”, “personal data”, “data controller” shall have the meaning ascribed to them in the UK Data Protection Act 1998 and, as of 25 May 2018, General Data Protection Regulation (EU) 2016/679.

2. The processing of personal data

- 2.1. The Data Controller warrants that it will process the personal data in accordance with the UK Data Protection Act 1998 and as of 25 May 2018 in accordance with the General Data Protection Regulation (EU) 2016/679 and any additional data protection laws which will come into effect in the UK.
- 2.2. The Data Controller warrants that it will process the personal data only in such a manner as - and to the extent that - this is necessary for the purposes of the EU H2020 STRENGTHS project.
- 2.3. The personal data will not be processed for other purposes.
- 2.4. The Data Controller warrants that it shall treat all personal data strictly confidential and that it shall inform all its employees and/or approved (sub-) processors engaged in the processing of personal data of the confidential nature of such information and of the personal data. The Data Controller shall ensure that all employees or other persons working with the personal data are bound to adequate confidentiality agreements.

3. Security

- 3.1. The Data Controller warrants that it shall implement appropriate technical, physical and organizational measures to ensure the security of the personal data. These measures shall include in any case:
 - (a) measures to ensure that the personal data can be accessed only by authorized personnel for the purposes of EU H2020 STRENGTHS project.
 - (b) measures to protect the personal data against accidental or unlawful destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure;
 - (c) measures to identify vulnerabilities with regard to the processing of personal data in systems used by the data controller.
- 3.2. The Data Controller shall at all times have in place a suitable, written security policy with respect to the processing of personal data, outlining in any case the measures set forth in 3.1.



3.3. The Data Controller acknowledges that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures.

Signature

A handwritten signature in blue ink, consisting of a large, stylized initial 'L' followed by a series of loops and a long horizontal stroke.

Name

Lucinda Parr

Title

Secretary & Registrar

Date signed

June 7, 2017



DATA PROTECTION LABEL War Child

The War Child, a foundation incorporated under the laws of the Netherlands, having its registered office and principal place of business in Amsterdam at Helmholtzstraat 61G, 1098 LE Amsterdam (hereinafter to be referred to as: the: "**Data Controller**") hereby warrants as follows:

1. Subject matter of this Data Protection Label

- 1.1. This Data Protection Label applies exclusively to the processing of personal data in the scope of the EU H2020 STRENGTHS project.
- 1.2. Terms such as "processing", "personal data", "data controller" shall have the meaning ascribed to them in the General Data Protection Regulation (EU) 2016/679.

2. The processing of personal data

- 2.1. The Data Controller warrants that it will process the personal data in accordance with the Dutch Data Protection Act (*Wet bescherming persoonsgegevens*, hereinafter : the "**Wbp** and as of 25 May 2018 in accordance with the General Data Protection Regulation (EU) 2016/679 and any additional data protection laws which will come into effect in the Netherlands.
- 2.2. The Data Controller warrants that it will process the personal data only in such a manner as - and to the extent that - this is necessary for the purposes of the EU H2020 STRENGTHS project.
- 2.3. The personal data will not be processed for other purposes.
- 2.4. The Data Controller warrants that it shall treat all personal data strictly confidential and that it shall inform all its employees and/or approved (sub-)processors engaged in the processing of personal data of the confidential nature of such information and of the personal data. The Data Controller shall ensure that all employees or other persons working with the personal data are bound to adequate confidentiality agreements.

3. Security

- 3.1. The Data Controller warrants that it shall implement appropriate technical, physical and organizational measures to ensure the security of the personal data. These measures shall include in any case:

(a) measures to ensure that the personal data can be accessed only by authorized personnel for the purposes of EU H2020 STRENGTHS project.

(b) measures to protect the personal data against accidental or unlawful destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure;

(c) measures to identify vulnerabilities with regard to the processing of personal data in systems used by the data controller.

3.2. The Data Controller shall at all times have in place a suitable, written security policy with respect to the processing of personal data, outlining in any case the measures set forth in 3.1.

3.3. The Data Controller acknowledges that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures.

Signature



Name

Agnès Kaijen

Title

Legal Advisor

Date signed

June 1st, 2017



DATA PROTECTION LABEL SEHIR

Istanbul Şehir University (ŞEHİR) is a non-profit foundation university based in İstanbul, Turkey. It was officially founded by the Foundation for Sciences and Arts in 2008 and currently resides in Kuşbakışı Caddesi No.27 34662 Altunizade Üsküdar/İstanbul address.

1. Scope:

1.1. This Data Protection Label applies exclusively to the processing of personal data in the scope of the project (*Fostering responsive mental health systems in the Syrian refugee crisis — STRENGTH - 733337*)

2. Definitions:

2.1. Terms such as express consent, personal data, processing of personal data, data processor, data supervisor, data subject, institution, data recording system, shall have the meaning ascribed to them in the Turkish Personal Data Protection Act with no. 6698. (*Kişisel Verilerin Korunması Kanunu*, hereinafter : the "KVK").

3. The processing of Personal Data

3.1. Istanbul Sehir University acts as the Data Supervisor.

The Data Supervisor warrants that the personal data shall only be processed only in such a manner as – and to the extent that - this is necessary for the purposes of the project (*Fostering responsive mental health systems in the Syrian refugee crisis — STRENGTHS - 733337*)

3.2. The Data Supervisor or the authorized person shall inform the Data Subject on the identity of the Supervisor or its representative, the purposes for which the personal data will be processed, the persons to whom processed personal data might be transferred and the purposes for the transfer, the method and legal cause of collection of personal data, the rights of the Data Subject.

3.3. The Data Supervisor warrants that all personal data will be treated as strictly confidential and inform all its employees and/or data processors engaged in the processing of the personal data of its confidential nature. The Data Supervisor shall sign confidentiality agreements with all employees and data processors working with the personal data.

4. Security

4.1. The Data Supervisor warrants that it shall take all necessary technical and organizational measures for providing an appropriate level of security in order to:

4.1.1. Prevent unlawful processing of personal data,

4.1.2. Prevent unlawful access to personal data,

4.1.3. Safeguard personal data.

4.2. The Data Supervisor shall carry out or have carried out necessary inspections within his institution and organization in order to ensure implementation of the provisions of the Turkish Personal Data Protection Act no.6698.

Prof. Dr. Peyami ÇELİKCAN
Deputy Rector
26.05.2017



Mülteciler ve Sığınmacılar Yardımlaşma ve Dayanışma Association (Refugees and asylum Seekers Assistance and Solidarity Association – RASASA)

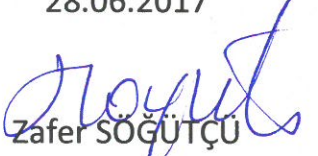
DATA PROTECTION LABEL RASASA

Rasasa is a non-profit association based in Istanbul, Turkey. It was established in 2014 to seek solutions to the problems of people who have left their country and are in need of international protection and currently resides in Turgut Reis Mah. Fatih Bulvarı, Postcode: 34930 No: 306 Sultanbeyli/İstanbul address.

1. Scope:
 - 1.1. This Data Protection Label applies exclusively to the processing of personal data in the scope of the project (Fostering responsive mental health systems in the Syrian refugee crisis – STRENGTH - 733337)
2. Definitions:
 - 2.1. Terms such as express consent, personal data, processing of personal data, data processor, data supervisor, data subject, institution, data recording system, shall have the meaning ascribed to them in the Turkish Personal Data Protection Act with no. 6698. (Kişisel Verilerin Korunması Kanunu, hereinafter : the "KVK").
3. The processing of Personal Data
 - 3.1. RASASA acts as the Data Supervisor.

The Data Supervisor warrants that the personal data shall only be processed only in such a manner as — and to the extent that - this is necessary for the purposes of the project (Fostering responsive mental health systems in the Syrian refugee crisis — STRENGTH - 733337)
 - 3.2. The Data Supervisor or the authorized person shall inform the Data Subject on the identity of the Supervisor or its representative, the purposes for which the personal data will be processed, the persons to whom processed personal data might be transferred and the purposes for the transfer, the method and legal cause of collection of personal data, the rights of the Data Subject.
 - 3.3. The Data Supervisor warrants that all personal data will be treated as strictly confidential and inform all its employees and/or data processors engaged in the processing of the personal data of its confidential nature. The Data Supervisor shall sign confidentiality agreements with all employees and data processors working with the personal data.
4. Security
 - 4.1. The Data Supervisor warrants that it shall take all necessary technical and organizational measures for providing an appropriate level of security in order to:
 - 4.1.1. Prevent unlawful processing of personal data,
 - 4.1.2. Prevent unlawful access to personal data,
 - 4.1.3. Safeguard personal data.
 - 4.2. The Data Supervisor shall carry out or have carried out necessary inspections within his institution and organization in order to ensure implementation of the provisions of the Turkish Personal Data Protection Act no.6698.

28.06.2017


Zafer SÖĞÜTÇÜ
Dernek Başkanı



DATA PROTECTION LABEL: University of New South Wales

University of New South Wales, Sydney, a foundation incorporated under the laws of New South Wales (University of New South Wales Act, 1989), having its registered office and principal place of business in Sydney, Anzac Parade, Kensington, NSW (hereinafter: the “**Controller**”) hereby warrants as follows:

1. Subject matter of this Data Protection Label

- 1.1. This Data Protection Label applies exclusively to the processing of personal data in the scope of the EU H2020 STRENGTHS project.
- 1.2. Terms such as “processing”, “personal data”, “controller” shall have the meaning ascribed to them in the General Data Protection Regulation (EU) 2016/679 (hereinafter: the “**GDPR**”).

2. The processing of personal data

- 2.1. The Controller warrants that it will process the personal data in accordance with the UNSW’s Recordkeeping Policy, Electronic Recordkeeping Policy, and associated procedures under the State Records Act 1988 (NSW), and as of 25 May 2018 in accordance with the GDPR and any additional data protection laws which will come into effect in New South Wales.
- 2.2. The Controller warrants that it will process the personal data only in such a manner as - and to the extent that - this is necessary for the purposes of the EU H2020 STRENGTHS project.
- 2.3. The personal data will not be processed for other purposes.
- 2.4. The Controller warrants that it shall treat all personal data strictly confidential and that it shall inform all its employees and/or approved (sub-)processors engaged in the processing of personal data of the confidential nature of such information and of the personal data. The Controller shall ensure that all employees or other persons working with the personal data are bound to adequate confidentiality agreements.

3. Security

3.1. The Controller warrants that it shall implement appropriate technical, physical and organizational measures to ensure the security of the personal data. These measures shall include in any case:

(a) measures to ensure that the personal data can be accessed only by authorized personnel for the purposes of EU H2020 STRENGTHS project.

(b) measures to protect the personal data against accidental or unlawful destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure;

(c) measures to identify vulnerabilities with regard to the processing of personal data in systems used by the Controller.

3.2. The Controller shall at all times have in place a suitable, written security policy with respect to the processing of personal data, outlining in any case the measures set forth in 3.1.

3.3. The Controller acknowledges that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures.

Signature:



Kate Carruthers

Chief Data Officer

Date signed: 5th June 2017



University of Zurich
Prof. Dr. med. Ulrich Schnyder
Department of Psychiatry and Psychotherapy
Culmannstrasse 8
CH-8091 Zürich

Zurich, 12 April 2017
Our Ref No: DSD17.01.21

**H2020 collaborative project
“Fostering responsive mental health systems in the Syrian refugee crisis”**

To whom it may concern

In my function as the Delegate for Data Protection of the University of Zurich I would like to make the following statement regarding the H2020 collaborative project “Fostering responsive mental health systems in the Syrian refugee crisis” (Acronym: STRENGTHS / EU contract number: 733337) headed by Prof. Dr. med. Ulrich Schnyder from the Department of Psychiatry and Psychotherapy:

I can confirm to the European Commission that the University of Zurich as a public authority of the Canton of Zurich is subject to mandatory cantonal data protection provisions and has internal regulations and procedures in place to ensure that applicable legal data protection provisions are being adhered to (<http://www.dsd.uzh.ch/de/law-collection.html>).

For this purpose Prof. Schnyder will provide the Department of the Delegate for Data Protection of the University of Zurich (<http://www.dsd.uzh.ch/de.html>) with the required documentation prior to the start of the project. The Department of the Delegate for Data Protection of the University of Zurich and where required as well the Data Protection Commissioner of the Canton of Zurich (<https://dsb.zh.ch/interneVdatenschutzbeauftragter/de/home.html>) will review the documentation and the procedures for the processing of personal data of the project in respect of compliance with applicable data protection provisions.

Sincerely

Universität Zürich
Datenschutzdelegierter der UZH

Dr. Robert Weniger
Datenschutzdelegierter