Data Protection Protocol and Guidelines for PHIT Project

1. General Protocol

This aim of the present protocol is to serve as a guide to the interviewers who will have access to personal data as part of the research project untitled “Psychological Health Impact of THB for sexual exploitation on female victims” (PHIT), taking into account the fundamental right of the interviewees to data protection, as set out below.

Project PHIT is coordinated by the University of Barcelona and funded by the European Commission and aims to “improve knowledge on the psychological impact of trafficking in human beings on victims and measure the impact of stakeholders’ interventions and interactions on the psychological wellbeing of the victims”. During the project, personal data1 will be collected and processed2 by members of the project team, and will be mainly obtained through in-depth semistructured interviews with former THB for sexual exploitation victims, through interviews and focus groups with professionals and experts in that matter and through a forensic analysis of the women’s health. More specifically, because of the research topic and the type of questions that will be asked, the interviewees will share in their answers a series of “highly sensitive data”, that refer to the most intimate area of their lives (ideology, health, sex life, ethnic background, beliefs, religion).

As a consequence, account is to be taken of the provisions of the personal data protection legislation, and especially the European legislation stated in the General Data Protection Regulation (GDPR), the Spanish Organic Law 15/1999 of 13 December on the Protection of Personal Data (OLPD) and its Development Regulation.

According to the provisions of the legislation previously mentioned, high-level technical and organisational security measures must be implemented and interviewees must be previously informed of the use of their personal data (art. 5.1 of the OLPD) and must give their consent to allow its processing by the members of the project team (art.6 of the OLPD).

---

1 Personal data: “Any information referring to identifiable or identified persons” (art. 3a OLPD) or “any numerical, alphabetical, graphic, photographic, acoustic or any other type of information referring to identifiable or identified persons”. (art. 5f ROLPD)

2 Data processing: “Any operation or technical procedure, automatic or non-automatic, that would allow the collection, recording, conservation, elaboration, modification, consult, use, cancellation, blockage, suppression or cessions of data that would result from communications, consults, interconnections and transfers”. (art. 3c OLPD)
Some guidelines that should be taken into account in the processing of personal data during the whole duration of the project are detailed below, as a guide to the members of PHIT project team who will be participating to data collection and data processing.

2. Data Protection Guide for PHIT Partners

2.1 Data collection during interviews and focus groups: key principles

- Even if the project team members are already subject to the obligation of professional secrecy, it is essential that all those participating to the processing of personal data read and sign the document untitled “Declaration of confidentiality” before the start of the interview / focus group.

- Before starting the interview/focus group, the “Informed Consent Form” must be provided to the participant (THB former victim or professional) so that he/she is informed of the provisions stated in the art. 5.1 of the Spanish Organic Law on the Protection of Personal Data and of all the other matters mentioned in the document.

- The consent of the participant for the processing of his/her personal data as part of the research project must be obtained through the signing of the “Informed Consent Form”. If the participant refuses to sign this document, the interview cannot be conducted.

- “Informed Consent Forms” signed by the participants must be kept in case they are required by Data Protection Authorities or requested by tribunals or judges to evaluate potential non-compliance with data protection legislation during the period of data processing and during its period of prescription. They must be sent to the Project Manager before March 2018.

- During the interview/focus group, interviewers must follow the interview protocol and must not ask questions other than the ones stated in the interview protocol.

- [Interviews with former victims] Answers and notes must be written on the file provided to conduct the interview. If notes are taken on paper, they must be kept in a secured restricted-access area and must be destroyed once the corresponding interview package has been uploaded to the platform.

- [Interviews with former victims] Interviews with former victims will be recorded. Interviewers must make sure to change the woman’s name during the whole interview, as a safety measure to protect her confidentiality.

- Data collected during the interviews can only be used for the purposes of this research project.

---

3 The original signed Declaration of Confidentiality of every person who has access to personal and confidential data collected as part of PHIT study (interviewer, interpreter etc.) must be sent to the project manager.
2.2 Data processing: safety rules

a. Interview transcripts

Account should be taken that once the information proceeding from the interviews has been collected, the anonymization\(^4\) technique should be applied. Interviews with victims should be transcribed in order to facilitate the analysis of the collected data. The anonymization technique will be applied to transcripts: every element or data that could allow the identification of the interviewee taking part to the study should be modified/alterd.

- For instance: specific places, physical characteristics, names...

b. Storage

Access control:

Only previously authorized staff must have access to data. Authorized staff must only have access to the data he/she needs to carry out his/her work, whether it is on an informatic or paper medium.

- Informatic mediums

  Sharepoint Platform

IT services of the University of Barcelona will implement a highly secured platform where partners will be able to store and share information and data. The access will be highly restricted and all the information it contains will be encrypted. A username and password\(^5\) will be assigned to each authorized person working with this data. This username and password are individual and confidential, they cannot be used by anyone else than the person they were created for. Each Partner (NGO, University...) will have access to a personal account within the secured platform. There, the authorized staff will be able to upload data and files (text and audio). It is strongly recommended to save interview material and transcription only in that platform, and not directly on your computer. If saved on your computer, we recommend you to encrypt those documents and to protect them with a password, containing at least one letter, one number and one symbol. Each user will have to inform the project manager of any incident or malfunction that could affect the safety of the personal data contained within the platform. They must also report any incident regarding the security of his/her username and/or password. The user will be held responsible of any consequence that could arise from misuse, disclosure or loss of his/her personal username and password.

---

\(^4\) Anonymization: “data processing resulting in making it impossible to identify one person without using additional information. This additional information must be kept separately and must be subject to technical and organizational measures aiming to guarantee that personal data cannot be attributed to an identifiable or identified person”. (Art. 4.5 RGPD).

\(^5\) Each authorized person who will have access to personal data will have to fill in a request form to obtain a personal and confidential username and password.
Audio files
[Interviews with former THB victims] As an additional measure of safety, the voice of the participant should be altered before uploading the audio file to the Sharepoint platform.

Computer security
Computers and other devices such as printers and scanners should be secured. Once partners have been assigned a username and password by the IT services, they will be able to download and install the antivirus SOPHOS on their computer, free of charge. It is essential to identify computers with which each person will work. It is strongly recommended to only use this computer. If you need to work on a portable device or outside of the partner premises, you will need a prior written authorization from the project director.

Data cancellation
Each time a medium or a document containing personal data must be destroyed or suppressed, it should be made in accordance with the measures implemented to prevent the access to the information contained or its subsequent recovery.

○ Paper mediums
If possible, please only keep the information and data on informatic mediums, and not on paper. It is easier to secure the content of the informatic medium on the highly-secured platform Sharepoint. If you are using paper-based documents (notes, answers to questionnaires), please make sure to follow the following guidelines.

Archiving and storage
Documents in paper must be kept in a restricted-access and closed area. They must be protected by mechanisms that prevent their opening by non-authorized staff (locks ...). Only authorized staff can have access to those documents.
Archiving of media or documents should be made while guaranteeing the proper conservation of the documents, its location, the possibility to consult the information it contains and the possibility to exercise the rights of objection to the processing, access, rectification and cancellation.
Partners must keep a record where is stated who has had access to the documentation, date and hour, and for which purpose.

Copies and data cancellation
Each time a medium or a document must be destroyed or suppressed, it should be made in accordance with the measures implemented to prevent the access to the information contained or its subsequent recovery.
Copies and reproductions might be made but with prior authorization from the Project Director.
Transfers
To send the data collected through interviews and focus groups, partners will be asked to use exclusively the secured platform that will be implemented by the University of Barcelona. The platform contains secured messaging systems (Yammer, Skype and secured email). **Partners must not send any data or confidential information through their professional or personal email.**

*Project PHIT is co-funded by the Internal Security Fund of the European Commission. This publication reflects the view only of the authors, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.*