Basic information about personal data collection and processing

1. **Personal data**

   Personal data is all information about an identified or identifiable natural person. In particular, personal data includes, but is not limited to: name, surname, gender, date of birth, PESEL number, tax number, address (including certain types of e-mail addresses), telephone number, IP address, geolocation data or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person.

   Special categories of personal data are data revealing racial or ethnic origin, political views, religious or philosophical beliefs, union membership, genetic data, biomedical data, medical history and sexuality or sexual orientation.

   Whether certain information constitutes personal data is determined by the context in which it is being processed. If, in a given context, the information does not allow to identify a particular natural person, it is not considered personal data.

   RECOMMENDATIONS: If you are going to collect personal data during the course of the study, the application to the Committee should include:

   - Information clause on personal data processing, and participant informed consent

   If you are going to collect information that falls under the special categories of personal data during the course of the study, the application to the Committee should include:

   - Information clause on personal data processing, and participant informed consent highlighting any issues relating to the collection and processing of special categories of personal data

2. **Anonymization and pseudonymization of personal data**

   Pseudonymization – reversible processing of personal data in such a way that the data can no longer be linked to a specific participant. The information necessary to reverse pseudonymization (which is usually a list that contains names and codes that make it possible to identify data sets coming from individual participants) should be stored in a way that prevents unauthorized access. Pseudonymization of data does not constitute anonymization. Pseudonymized data still remain personal data.

   Anonymization - irreversible processing of personal data in such a way that the data can no longer be linked to a specific participant by, for example, replacing data with random characters or ID numbers that cannot be traced back to individual participants.

   RECOMMENDATIONS: All interviews, recordings, photographs or other documents should be anonymized as soon as possible, ideally at the very moment of data collection. One should limit the collection of personal information to what is directly relevant and necessary to the study. In many cases there is no need of linking individual data sets to personal data of participants that the results came from. The Committee recommends, if possible, that personal data should not be collected or that non-anonymized data should be deleted as soon as possible. This does not concern studies where researchers plan to inform participants about their individual results, longitudinal studies, etc.

3. **Establishing all objectives for personal data processing**

   RECOMMENDATIONS: It is essential to always establish **all objectives for personal data processing**. All information about the aims of the study, the people and entities who will have access to the data, as well as what the data will be used for, must be included in the information on the collection and processing of personal data:

   a) The data obtained during the study may only be used for purposes specified in the information on the collection and processing of personal data and as described in the participant consent on personal data processing.
   b) The data obtained during the study cannot be shared with any entity that have not been listed in the information, nor can it be used for any other research that the participants have not consented to (if you wish to use previously collected data, you must obtain re-consents from the participants).

4. **Data minimization**

   The **data minimization** principle implies the obligation to limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. At the same time, the principle of storage limitation entails a responsibility to erase data as soon as the they cease to be useful for the purposes of processing. This means that processing personal data beyond the minimum necessary will constitute a violation of data protection.

   RECOMMENDATIONS: The application (point 3a) should also include information on how long you are planning to retain participants' personal data and how they will be stored (this also applies to informed consent forms for participation in the study and data processing consent forms). This information should also be included in the documents handed to participants.

   How long should I store data?

   RECOMMENDATIONS: The information included in the informed consent forms should be processed for as long as you are processing the data during the study and, after it is completed, until the statute of limitations for any civil law claims expires. However, after the study has been completed, data may be stored **only to defend yourself against any possible claims**. Similarly, any transcriptions, audio/video recordings, photographs, medical records, etc. should be kept until the research project is completed and results are presented in a paper or the project is documented in a different manner.

   Anonymized data can be used freely and stored indefinitely, as it is no longer personal data under the GDPR provisions. Therefore, any kind of interviews, recordings, photos or other documentation **should be anonymized as early as possible**.

Useful resources

1. Regulation of the European Parliament and the Council (EU) 2016/679 of April 27, 2016 on protection of individual persons with regard to the personal data processing and on the free flow of such data, and also repealing Directive 95/46/EC (general regulation on data

protection) (Polish) https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32016R0679&from=PL#d1e40-1-1

2. Data Protection Officer (DPO) https://odo.uw.edu.pl/kontakt/