EASHW TIPS – RECORDINGS (WITH IDENTITY INFORMATION)

C12. RECORDINGS: DO YOU MAKE OR COLLECT RECORDINGS OF PEOPLE, AND DO YOU SAVE THEM DURING OR AFTER THE DATA ANALYSIS?

Recordings can make people identifiable. For instance, audio recordings are identity information, as every voice is unique. Both ETHICAL CONSENT AND LEGAL (GDPR) CONSENT are required when making or using recordings, as these qualify as identity information.

Both ETHICAL CONSENT AND LEGAL (GDPR) CONSENT are required for all types of **recordings that can qualify as identity information directly and indirectly**. Photos, audio- and video recordings fall under this category, but also other recordings may qualify as identity information. Here are some additional examples and considerations for what might fall under this category, and require to be handled according to the GDPR-legislation:

- DIGITAL INTERACTIONS: Screen recordings, chat logs, or online activity (e.g., social media usage patterns) need to be treated as identity information if these interactions include identifiable data or behaviors unique to a participant.
- ENVIRONMENTAL RECORDINGS: Recordings of a participant's home or workplace (e.g., video of their environment as part of a research method) need to be treated as identity information if the environment or objects in the recording make it possible to identify the participant indirectly.
- BIOMETRIC RECORDINGS (brain wave recordings (EEG), heart rate (ECG), fingerprints, facial recognition scans, iris scans, etc.) may qualify as identity data under GDPR. The European Data Protection Supervisor states that "neurotechnologies are able to infer individuals' physical health or fitness and mental state (e.g. problem-solving, reasoning, decision-making, comprehension, memory retrieval, perception, language, emotions). It is therefore a very intrusive, if not the most intrusive processing, encroaching upon the very mental privacy and possibly mental integrity of the person concerned." (see https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2024-06-03-techdispatch-12024-neurodata_en) We therefore advice all researchers using biometric recordings to answer "YES" to question 12 and take the required precautious measures.
- BEHAVIORAL RECORDINGS: if the pattern or behavior is unique enough to identify an individual, then answer YES to question 12.

Both ETHICAL CONSENT AND LEGAL (GDPR) CONSENT are required for:

1. All recordings that can qualify as identity information directly and indirectly **made by researchers** (e.g., interviews, observations).
2. All recordings that can qualify as identity information directly and indirectly **provided by participants** (e.g., photovoice projects, personal archives).

THE ETHICAL RISK **increases if recordings are retained during or after data analysis**. If all recordings are permanently deleted after anonymous transcription and before analysis begins, you may answer "NO" to question 12. However, if recordings are used during analysis or saved for later (re)use, answer "YES."

When making recordings, the GDPR LEGISLATION applies and must be complied with. If in doubt about GDPR-related aspects, it is best to contact the Privacy Commission (privacy@uantwerpen).

For question 12 about recordings, the following answer options are:

- YES to question 12 = recordings with identity information are **made or collected AND retained** during or after data analysis. In this case, the following list of questions needs to be addressed.
- NO to question 12 = recordings with identity information are **made or collected BUT NOT retained** during or after data analysis. In this case, the following list of questions needs to be addressed.
- NA to question 12 = **NO recordings** with identity information are made or collected.

This document outlines what you need to explain in your answer (YES or NO). At the end, we address when recordings in public settings may be made without explicit consent.

YES TO QUESTION 12

YES to question 12 = recordings are retained during or after data analysis. In this case, the following list of questions needs to be addressed:

1. WHAT recordings of people do you take or obtain?
   - Specify the type of recordings and their purpose. Will you make or collect photos or video-, or audio recordings? Or any other types of recordings that may qualify as identity information according to the GDPR. See the information above.
   - Keep in mind: Recordings that involve identity data increase ethical risks and requiring explicit GDPR-compliant consent.
2. WHERE do you keep the recordings safe? (This must be on secure AUHA servers. If you (temporarily) deviate from this: motivate why)
   - Data in which individuals are identifiable are only stored on secure AUHA servers or applications (N drive, Teams, OneDrive for Business, SharePoint).
   - If this is temporarily not possible, data is stored on a personal carrier that is protected with a password, two-step verification and/or encryption program such as 7-Zip or AEScrypt.
   - Never use Google Drive, Dropbox, WeTransfer, personal OneDrive, or other non-AUHA systems to share data.
   - In Part B of the EASHW application you are also asked to guarantee that you will always treat identity information in accordance with these guidelines and the GDPR-legislation. This also applies to the use of recordings with identity information. Do not break that promise.
3. HOW long do you keep the recordings?
   - State the retention period and justify why recordings are kept for that duration.
   - GDPR requires identity data to be stored only as long as necessary. Keeping recordings indefinitely increases risks to participant privacy.
4. WHO has access to the recordings?
   - List everyone with access (e.g., researchers, assistants) and their roles.
   - Participants have the right to know who can view their identity data; you must also mention this information in the informed consent.
   - Limiting access reduces risks of misuse or breaches.
   - Make sure that everyone with access signs a CONFIDENTIALITY AGREEMENT, and ensure these documents are attached to your application.
5. DO you share the recordings with third parties? If so, with whom and why?
   - Data in which individuals are identifiable (including recordings) can only be shared:
     - With persons/institutions of which those involved have been informed;
     - With the consent of those involved;

- Through secure channels. If possible, files are encrypted with a password or code. You can send large files via Belnet Filesender (https://filesender.belnet.be/).

- In Part B of the EASHW application you are also asked to guarantee that you will always treat identity information in accordance with these guidelines and the GDPR-legislation. This also applies to the use of recordings with identity information. Do not break that promise.

6. DO/WILL you publish images or fragments? If so, through which channels?
   - Specify IF, WHERE, AND HOW recordings will be SHARED PUBLICLY (e.g., academic journals, presentations).
   - All people of whom recordings are being made public must give explicit and fully informed consent for publication.
7. Do the persons concerned give SEPARATE EXPLICIT CONSENT for:
   a. MAKING the recordings?
   b. STORING the recordings (where, for how long, by whom)?
   c. SHARING the recordings (how, with whom)?
   d. PUBLISHING images or fragments?
   - In the INFORMED CONSENT:
     - Clearly define the recordings that will be used and do this in simple terms. This ensures participants understand what is being captured. Ambiguous or broad consent can lead to breaches of privacy and legal non-compliance.
     - The above listed types of consent must be presented and recorded separately (separate tick boxes). Participants have the right to agree only with some options; e.g. they may agree with the making and storing or recordings but not with the sharing and publishing.
     - PLEASE NOTE: Please only use relevant and CUSTOMIZED CONSENT OPTIONS from our website's informed consent forms. Unclear, missing or redundant information in the informed consent forms will result in a PRELIMINARY NEGATIVE ADVICE from EASHW.
   - Use the INFORMED CONSENT TEMPLATE FOR NON-ANONYMOUS RESEARCH.
   - This template includes only the minimum required information as per EASHW and GDPR standards. While you must adapt the language to suit your target population, the content itself cannot be changed.

NO TO QUESTION 12

NO to question 12 = recordings with identity information are made or collected BUT NOT retained during or after data analysis. In this case, the following questions need to be addressed.

1. WHAT recordings of people do you take or obtain?
   - See information above to check if the recordings you plan to use can best be considered as identity information according to the GDPR.
   - Keep in mind: Recordings that involve identity data increase ethical risks and requiring explicit GDPR-compliant consent.
2. CONFIRM that all recordings are permanently deleted before data analysis.
   - State the retention period and also mention this in the informed consent.
3. Do the persons being recorded give SEPARATE EXPLICIT CONSENT for:
   1. MAKING the recordings?
   2. The TEMPORARY STORAGE of the recordings (where, for how long, by whom)?
   - In the INFORMED CONSENT:

- Clearly define the recordings that will be used and do this in simple terms. This ensures participants understand what is being captured. Ambiguous or broad consent can lead to breaches of privacy and legal non-compliance.
- The consent for making and temporarily storing the recordings must be presented and recorded separately (separate tick boxes).
- PLEASE NOTE: Please only use relevant and CUSTOMIZED CONSENT OPTIONS from our website's informed consent forms. Unclear, missing or redundant information in the informed consent forms will result in a PRELIMINARY NEGATIVE ADVICE from EASHW.

- Use the INFORMED CONSENT TEMPLATE FOR NON-ANONYMOUS RESEARCH.
- This template includes only the minimum required information as per EASHW and GDPR standards. While you must adapt the language to suit your target population, the content itself cannot be changed.

NA TO QUESTION 12

NA to question 12 = NO recordings with identity information are made or collected.

- **If you make any recordings that do not entail any identity information**, please explain and argue why they should not be considered as identity information according to the GDPR.

RECORDINGS IN PUBLIC SPACES

- Recording people in public spaces is allowed but **must be disclosed**.
- **Announce recordings in advance** whenever possible, especially if the recording process is not obvious.
- **If someone objects** to being recorded or recognizable, **stop recording and delete any material** where that person is identifiable.
- Use recordings **strictly for scientific purposes** and do not share them beyond the research context (e.g., *avoid sharing during presentations*).
- Respect individual preferences, even in public spaces—some people may not want to be identifiable.

INDIRECT DATA SUBJECTS IN RECORDINGS

- Recordings may involve others indirectly.
  - For example, bystanders in photo/video recordings or people overheard in audio recordings.
  - In photovoice projects, participants may capture images or discuss others during research.
- **Minimize indirect involvement** whenever possible.
  - Conduct recordings in spaces where only participants are present.
  - If participants make recordings:
    - Ask participants not to capture other people if possible.
    - When they do record other people, ensure they offer them the **opportunity to consent (or decline) to their indirect involvement.**