### **DATA PROTECTION CONSIDERATIONS FOR YOUR RESEARCH PROJECT, THESIS, OR DISSERTATION**

1.1 It is recommended that any personal data collected in the course of preparing your Research Project, Thesis, Dissertation, or Presentation should be **anonymised**. For example, if you have used a survey to gather responses, you can anonymise the data by securely deleting the name or any other identifying data from the dataset. It should never be possible to attribute survey responses to an individual after anonymisation.

* 1. Where anonymisation is not possible, you can **pseudonymise** the data. This means that you remove obviously identifying information from the dataset e.g. name or identification number. This identifying information should be kept separately to the main dataset. The identifying information should be protected (e.g. kept in a password protected file) and only be accessible by the student researcher.

1.3 Where anonymization or pseudonymisation is not possible from the outset you should answer the following questionnaire and adhere to the guidelines provided in this document.

1.4 Where there is an intention for the final publication to reference actual personal data and/or special category personal data you should contact the Information and compliance office at dp@ait.ie.

|  |  |
| --- | --- |
| **PERSONAL DATA ASSESSMENT QUESTIONNAIRE** | |
| a) Does your research require you to collect personal data? | \* |
| b) Will you be interviewing people? | If Yes – go to c) |
| c) Will the questions compel participants to reveal personal or sensitive (special category) data? | \* |
| d) Will you be conducting a survey? | If Yes – go to e) |
| e) Will the survey collect personal data? (Name, I.D, Email, Contact Details, I.P. Address) | \* |
| f) Are you collecting data from u-18’s | \* |
| g) Will you be assessing existing documentation which may contain personal data? | \* |
| h) Are you collecting the personal data from someone other than the data subject (person whose the information relates to)? (see note on permission) | \* |
| NOTE: Data can only be collected from a person other than the data subject with the express permission of the data subject. | |
| \*If you answered yes to any of the questions marked with an asterisk please follow the guidelines below. | |
| Acknowledgements Learners should consider the level of personal data they wish to include in the acknowledgement section of their publication. This may be done as an appreciation for the support of staff, family, and friends. It is general good practice to ask permission to make this inclusion. | |
| Personal data processing GUIDELINES2.1 List of Personal Data Make a list of each item of personal data you may require – e.g: Name; DoB; Email address; PPSn; Contact Details; Gender; Religious Beliefs, Health data…. Etc. 2.2 The reason why. Record a purpose for each item of personal data you require for this project. The purpose must be lawful, fair (have a valid reason); and transparent (no hidden agendas). If you don’t have a lawful purpose for each specific piece of data then you should not be collecting it. See point 2.6. 2.3 How much do you actually need? Look at each piece of data to see if you require it all. Minimise the data you collect as much as possible. E.g: Do you need someone’s age and date of birth; address and eircode? 2.4 Where are you getting the personal data from? Is the data subject providing the data or are you collecting it from a different source? If you are getting it from a different source – do you have permission to collect it and do they have permission to share it? Put in line that says ‘*I only want this information if you have permission to give it to me’* or *‘Please make sure you have permission to give this information’* **2.5 how are you collecting consent?**  1. In the majority of cases, collecting data for Research, Thesis, Dissertations, etc., will be based on consent or explicit consent. This is the ‘Lawful basis’ criteria referred to in points 2.6 and 2.7 below. 2. It will be important for you to have a recorded method of collecting data subject (individuals) consent for the processing of their data. This can take the form of a consent tick box on surveys or documentation. 3. ***Explicit consent*** should be in the format of a signed declaration. 4. Explicit Consent is required for all health related research and Special Category data (as listed in point 2.7). 5. You should provide the details of how the information will be processed at the same time as you are requesting consent. 6. Data collected as part of an anonymous survey still requires consent at the point of collection 7. Where consent is the sole basis for collection, it must be possible for the data subject to remove consent freely so that processing is stopped from that point forward.  2.6 On what Article 6 (Lawful) basis are you collecting the personal data? Where the data is being collected under any basis other than consent, please contact [dp@ait.ie](mailto:dp@ait.ie). Bases for collection are:   1. **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose. Must be as easy to withdraw as it was to give. 2. **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract. 3. **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations). 4. **Vital interests:** the processing is necessary to protect someone’s life. 5. **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. 6. **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)   **2.6.1 When collecting the information it is necessary to advise the data subject of:**   1. How the personal data will be collected. 2. Purpose of collection of the personal data 3. How long you will keep it 4. How securely you will keep it 5. How you will dispose of it 6. If you will be using the data in an anonymous format for your publication.  2.7 Is special category data being collected? The following items of personal data are listed as special category data and should not be processed unless they come under one of the bases listed under Article 9 of the GDPR (see point 2.7).   1. Race and ethnic origin. 2. Religious or philosophical beliefs. 3. Political opinions. 4. Trade union memberships. 5. Biometric data used to identify an individual. 6. Genetic data. 7. Health data. 8. Data related to sexual preferences, sex life, and/or sexual orientation.   If yes, why is this required? 2.8 On what Article 9 (Lawful basis for special category data) basis is this being collected? Where the data is being collected under any basis other than explicit consent, please contact [dp@ait.ie](mailto:dp@ait.ie). Bases for collection are:   1. **Explicit Consent:** Must have freely given the consent and you must be able to prove that consent was given and that it was given without coercion. Must be as easy to withdraw as it was to give. 2. **Vital Interest of the DS:** the processing is necessary to protect someone’s life. 3. **Manifestly made public by the DS:** The information has already been released in to the public arena **by the data subject.** 4. Employment/Social Security – rights of controller or DS 5. Legitimate activities of a not for profit organisation of whom the DS is a member  2.9 Where will you store the personal data?  1. Consider where you are storing the personal data. Hard copies should be scanned and stored on a password protected file on a PC/Laptop, or on a password protected PC/Laptop with authorised person access only. 2. Soft copies should be stored on a password protected file on a PC/Laptop or on a password protected PC/Laptop with authorised person access only. The original hard copy should be shredded. Where it is necessary to retain the hard copy, it should be stored in a secure filing cabinet. 3. You must have a high level of security (such as encryption) on your Laptop if using it to store personal and sensitive personal data. 4. It is not recommended that USB keys (unencrypted) be used to store personal data. 5. Data stored on the ‘Cloud’ generally has an encryption key to protect it against cyber-attacks, however each Cloud provider has different levels of encryption key protection. You will need to ensure that the security your provider has is sufficient to protect your data. Advice on this can be sought from the Institute’s IT Department.   **VIDEO AND VOICE RECORDINGS**   1. Video or voice recordings of interviews or other research methods should be retained only until the transcripts of the recordings have been completed. 2. Where the recordings are not being transcribed they should be retained only for the duration of the purpose of collection. A legal basis must be provided for the retention and this must be explained to the data subjects. 3. Where possible all personal data should be replaced by anonymous identifiers (e.g. Participant 1, 2, 3…). 4. The data must be stored securely, using password protection on files, and electronic devices. Hard copy or recordings must be securely locked away and accessible only to authorised personnel. 5. A defined and lawful retention period must be applied and adhered to.  2.10 Are you sharing the personal data with anyone else? Internal? External? When sharing personal data the following should be taken in to account:   1. Is the data being shared with the knowledge of the data subject and within the purpose for which the data was originally collected?    1. Data shared for another purpose will require additional consent. You should collect consent for all purposes at the point of first collection, otherwise a new consent to use will be required. 2. Where different bases are required for different processing, each basis must be noted. If consent is required then it must be collected at the point of collection of the data for that purpose. Different bases can be collected at the same point where the same set of data will be used. 3. It is important that the data subject knows who has access to the data and who will be processing it.  2.11 How long are you retaining the data? Why? Data must be held for the duration of the purpose for which it was collected. It may then be anonymised\*, pseudonymised\*, or deleted. The data subject must be given the details of the retention (how long it is being kept) the method of processing and how the personal data will be removed from the set of collected data  \**See examples on page one.* 2.12 How are you deleting/disposing of the data? Record the method of deletion/destruction of the data. The Institute uses confidential shredding bins. Discuss this with your supervisor, lecturer, or Faculty where appropriate. 2.13 Are you processing children’s data (u-18), or vulnerable adults? If yes, parental / guardian consent will be required for processing based on consent and additional safeguards will be required.  You will also need to get assent from the child or vulnerable adult.  Contact [dp@ait.ie](mailto:dp@ait.ie) for further advice. 2.14 Are you taking pictures oF data subjects or recording data subject interviews or activities? If yes, you will need to follow the TUS guidelines on the use of video or photographic content. These are available on the website at [www.ait.ie/gdpr](http://www.ait.ie/gdpr) or on request from [dp@ait.ie](mailto:dp@ait.ie). further information For further information or to ask a question, please contact the Information and Compliance office, TUS Midlands.  Email: [dp@ait.ie](mailto:dp@ait.ie)  Tel: 090 6468009  Website: [www.ait.ie/gdpr](http://www.ait.ie/gdpr) | |