**RESEARCH DATA PROTECTION IMPACT ASSESSMENT**

You should complete this assessment template if you are conducting a research project at Manchester Metropolitan University which involves the use of personal data[[1]](#footnote-1), and have been directly prompted by EthOS or by the Data Protection team that it is a requirement.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Principal Investigator owning research data** | Name:  Email Address: | | | |
| **Department/ Centre** |  | | | |
| **Project Title** |  | | | |
| **Status** | Staff | Doctoral researcher | Postgraduate | Undergraduate |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Data Protection Training** | | | | |
| The University is responsible for complying with the General Data Protection Regulation whenever personal data is processed. Under the Data Protection Policy, all staff and students have a responsibility to comply with the regulation in their day-to-day activities. The first step you can take to understand these responsibilities is to complete the University’s Mandatory Data Protection Training. Data protection training is available on the intranet data protection pages ([please follow this link](https://mmuintranet.mmu.ac.uk/Interact/Pages/Content/Document.aspx?id=2457&SearchId=)), and student training available through the Student Resource area in Moodle (in the ‘Skills Online’ section – [please follow this link](https://moodle.mmu.ac.uk/course/view.php?id=36&section=5)). To make sure your knowledge is up to date, all staff and students must complete the training every two years. If you have any issues in accessing the data protection training or have any questions about the training, please contact [dataprotection@mmu.ac.uk](mailto:dataprotection@mmu.ac.uk). | | | | |
| **I confirm that I have completed the Data Protection Training in the last two years (please tick)** | | | |  |
|  |  | | | |
| **High Risk Processing** | | | | |
| Does the research that you are conducting include any of the following (please tick all those that apply): | | | | |
| **High risk indicator** | | **Guidance note** | **Checkbox** | |
| a) Large Scale processing of sensitive special category[[2]](#footnote-2) data, or data of a highly personal nature | | *The factors to be considered when determining as to what extent constitutes ‘large-scale’ are: a) the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; b) the volume of data and/or the range of different data items being processed; c) the duration, or permanence, of the data processing activity, and d). the geographical extent of the processing activity*  *Research reviewing special category data from a large number of data subjects on social media platforms would meet this definition.* |  | |
| b) Processing of data relating to criminal convictions and offences | | *Using any identifiable data within your research that relates to an individual’s criminal history.* |  | |
| c) Processing of data concerning vulnerable individuals | | *Individuals can be vulnerable where circumstances may restrict their ability to freely consent or object to the processing of their personal data, or to understand its implications. This may include children, the elderly, or those with certain disabilities.* |  | |
| d) Use of MRI images or MRI data | | *Research that involves use of Magnetic Resonance Imaging (MRI) or data generated using MRI.* |  | |
| e) Systematic monitoring of a publicly accessible place on a large scale | | *This may include monitoring of CCTV cameras, use of drone recordings or video or audio recording in public spaces.* |  | |
| f) Processing involving the use of innovative technologies, or the novel application of existing technologies (such as Artificial Intelligence, Internet of Things (IoT), or location tracking) | | *This may include the use of Artificial Intelligence, Internet of Things (IoT), or location tracking. It may also apply to the novel use of these or other technologies.* |  | |
| g) Processing of biometric or genetic data | | *Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.*  *Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data.* |  | |
| h) Matching or combining data sets from more the one source | | *This may include combining data originating from two or more different studies or activities performed for different purposes. When combined, the data sets give a fuller picture of an identifiable data subject, in a way likely to exceed the reasonable expectations of the data subject. For example, combining information gathered from interview/ survey with information gathered from social media.* |  | |
| i) The processing of personal data which could result in a risk of harm to the data subject in the event of a security breach | | *‘Harm’ can mean physical, material or non-material damage, in particular: where a breach of the information may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality or embarrassment. It can also refer to personal data protected by professional secrecy, or data that may lead to significant economic or social disadvantage in the event of unauthorised disclosure.* |  | |
| j) Processing personal data without providing a privacy notice or participant information sheet directly to the individual | | *Also referred to as ‘invisible processing’, where the researcher considers that to provide this information would be impossible, or involve disproportionate effort.* |  | |
| k) None of the above | | *Please tick if none of the above statements apply to the proposed processing* |  | |
| **Please contact dataprotection@mmu.ac.uk if you are not sure if any of the above applies to your research project.** | | | | |
|  | | | | |
| **If you have ticked that any indicators from a) to g) apply above, then it is mandatory to conduct a Data Protection Impact Assessment (DPIA). Please complete the rest of this template and send it to** [**dataprotection@mmu.ac.uk**](mailto:dataprotection@mmu.ac.uk)**.**  **Where you ticked that none of the indicators apply (h), you do not need to complete the remainder of this template, but you must retain the record of having conducted the screening assessment.** | | | | |

**ASSESSMENT**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **DPIA Requirement** | | | | | | | | | | | | |
| * Provide an overview of your proposed research project. You may find it helpful to refer or link to other documents here. | | | | *Imagine you are explaining your project to someone who doesn’t know anything about the subject area.* | | | | | | | | |
| * Outline the reason why the DPIA has been required (refer to the initial screening evaluation) and what part it plays in the overall research project. | | | | *Which conditions from question 2) in the research evaluation were met? Why do they apply?* | | | | | | | | |
|  | | | |  | | | | | | | | |
| 1. **Processing of personal data** | | | | | | | | | | | | |
| **The Processing Lifecycle** | | | | | | | | | | | | |
| * Outline the purpose and benefits of the processing. | | | | *Why are you conducting this research? Who will it benefit and why?* | | | | | | | | |
| * How will you will collect, use and store the personal data. | | | | *Detail the data collection techniques – are you using primary or secondary data? If secondary data, where are you getting it from? Are you using qualitative or quantitative methods? Please provide details. How will you review the data? How will you store the data?* | | | | | | | | |
| * Describe the personal data you intend to process. Does it contain special category data or data relating to criminal offences? | | | | *In relation to personal data, ‘processing’ means 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, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction).* | | | | | | | | |
| * Outline the number of data subjects and scope of data collection (e.g. how often are you collecting data, what is the geographical area?). | | | | *Are you collecting data at multiple stages? How many data subjects will be involved? Where do the research population reside?* | | | | | | | | |
| * Describe how you will keep the data secure: Who needs to have access to the data; how will access control be managed; what other information security arrangements are there. | | | | *For example, are you using technical or physical security measures to protect the data at rest and in transfer? Pseudonymisation techniques, encryption, use of the Research Data Storage solution, lock and key for physical files etc.* | | | | | | | | |
| **Will you be using externally based storage for the research data?**  If you answer ‘yes’ please state how data will be stored:  <<<Type response here>>> | | | | | | | | | Yes | | | No |
| **Does the classification of the research data attract a marking of SECRET or above according to the HMG Classification scheme? (yes/no) –**  If you have answered ‘yes’ please state the marking:  *<<Type response here>>* | | | | | | | | | Yes | | | No |
| **If you have answered ‘yes’ to either of the above questions, you must ensure you contact** [**infosecurity@mmu.ac.uk**](mailto:infosecurity@mmu.ac.uk) **to make them aware of your proposal.** | | | | | | | | | | | | |
| **Please confirm you have contacted information security (yes/ no/ not applicable)** | | | | | | | Yes | No | | | | N/A |
| * Are personal data being shared outside of Manchester Metropolitan, or with Manchester Metropolitan? If so, who with, and why? Please also stipulate which country they are based in. * If you are sharing or transferring personal data or special category personal data outside of Manchester Metropolitan University to another organisation or individual, a data transfer agreement may be required. Please contact RKE contracts (RKE-Contracts@mmu.ac.uk) or Data Protection (dataprotection@mmu.ac.uk) to discuss this requirement. * Are you using an application service provider such as Survey Monkey, Qualtrics, Zoom or Padlet? Please specify if personal data will be provided and processed through these platforms, and the reasons for this. | | | | *Are you sharing with another organisation, or is another organisation sharing data with you? For example, the NHS, council, other University or policing organisation. Are you using a service provider where you will need to provide identifiable personal data to them, such as a transcription or translation service? Why is this necessary? Will personal data be transferred outside of the UK? If so, where?* | | | | | | | | |
| **It is your responsibility to ensure that appropriate sharing agreements are in place prior to the sharing taking place. Have you discussed any personal data sharing with RKE Contracts or the Data Protection team?** | | | | | | | | | | | Yes | No |
| * How long will the personal data be retained for? Will all the data be retained for the same amount of time? Please ensure you justify this retention period. | | | | *Please review the university’s* [*retention and disposal schedule*](https://www.mmu.ac.uk/records-management/retention-and-disposal-schedule/) *to help determine the retention period. Will data be anonymised and uploaded to the repository indefinitely after the project closes? Please note, data must always be anonymised prior to uploading to the University’s research repository.* | | | | | | | | |
| * Please specify who will have responsibility for ensuring this retention is met | | | | *Will you be with the University after the retention ends? If not, specify who you will pass this responsibility onto.* | | | | | | | | |
| **Has a Data Management Plan been completed for the project data? It is your responsibility to ensure that this is completed prior to the project commencing. The library has guidance on Research Data Management Plans,** [**available here**](https://libguides.mmu.ac.uk/rdm/dmp)**. Further information is available on** [**MMU’s website**](https://www.mmu.ac.uk/library/staff-and-researchers/research-data-management)**. Please contact rke-systems@mmu.ac.uk (RKE systems) or** [**rsl@mmu.ac.uk**](mailto:rsl@mmu.ac.uk) **(Library's Research Support Librarians) if you have any questions about the DMP.** | | | | | | | | | | | I confirm that a DMP has been completed | |
| **The context of the processing** | | | | | | | | | | | | |
| * How will you recruit the data subjects/ research participants? | | | | *How will you advertise your project and give people the choice on whether they would like to participate? If you are using secondary data sets, how will you choose this data?* | | | | | | | | |
| * How much control will the data subjects/ research participants have in how their data is used? | | | | *Will you provide granular options as to how their data are to be used, by using an informed consent form, for example? If you aren’t able to offer any flexibility, please specify why.* | | | | | | | | |
| * Do the data subjects/ research participants include children or other vulnerable groups? | | | | *Please consider ‘children’ to be anyone under 18. Please specify the age range of the participants if children are involved in the study. A vulnerable group includes persons who may be incapable of understanding what it means to participate in research. Individuals considered vulnerable may have a diminished capacity to anticipate, cope with, resist, and/or recover from the impact of a natural or man-made hazard. Vulnerable groups may also consist of individuals who are unable to care for themselves and/or may have an increased chance of suicide, self-harm, or the likelihood of harming others.* | | | | | | | | |
| * Are there any prior concerns over this type of processing or known security flaws? Is the research novel in any way? Does it use advanced technologies? Are there any current issues of public concern that you should factor in? | | | | *Is this type of research particularly sensitive, or has it had negative media coverage recently? Are the research methods cutting edge, little understood or particularly intrusive?* | | | | | | | | |
|  | | | |  | | | | | | | | |
| 1. **Consultation process** | | | | | | | | | | | | |
| * Explain any stakeholder engagement that has taken place to help shape your study (for example, would it be appropriate to consult a public group about your proposal, or conduct a pilot study? Have you sought any views of any IT or data protection specialists, academic experts, or used past studies to prompt your methods? If you would like further advice about information security measures, please contact [infosecurity@mmu.ac.uk](mailto:infosecurity@mmu.ac.uk). | | | | *If you have spoken to any data protection professionals, IT security professionals or research specialists, please give details here and summarise the advice given and whether you will follow it. Have you conducted any pilot studies, or are you using a similar study to prompt methods? Please give details.* | | | | | | | | |
| * If no stakeholder engagement has taken place, explain why it was not appropriate to do so. | | | | *Please list any reasons for not consulting – do you not feel that it would be appropriate given the nature of the study ? If not, why?* | | | | | | | | |
|  | | | |  | | | | | | | | |
| 1. **Necessity and proportionality** | | | | | | | | | | | | |
| What is your lawful basis for the processing? | | | | As a public authority acting in the public interest we rely upon the ‘public task’ lawful basis. When we collect special category data (such as medical information or ethnicity) we rely upon the research and archiving purposes in the public interest lawful basis.  *Please note: In some instances, we rely on ‘consent’ and ‘explicit consent’ (for sensitive special category data) as a lawful basis. This would usually apply where researchers take photographs of, or video individuals, as well as in some other instances. Where you rely on consent, you must ensure that you provide the participants with a separate release form, which states you are using ‘consent’ (and ‘explicit consent’, if required), as a lawful basis, and provides detail on how individuals are able to withdraw consent at any point (even after the data has been collected and processed). Please also make sure this lawful basis is recorded in this section of the assessment.* | | | | | | | | |
| Do you need to process personal data to meet the purpose of the research? Why can’t anonymised data be used? | | | | *Why aren’t you able to use anonymised data for your research? Why do the participants need to be identifiable?* | | | | | | | | |
| How will you ensure data minimisation? (i.e. how have you determined that the level of personal data being collected is proportionate to your purpose for research?) | | | | *Can each piece of personal data you collect be justified? Please explain how here. You should never collect personal data ‘just in case’. Have you considered anonymising early on in the research, or asking participants to provide anonymous returns to survey for examples?* | | | | | | | | |
| How will you tell the data subjects/ research participants about the processing? How will you ensure they read the Participant Information Sheet (PIS)? Are you using any other methods to provide this type of information? | | | | *At what point is the Participant Information Sheet being provided? Are you using several different PIS documents? If collecting personal data indirectly (i.e. not directly from the participants, via social media or other public source for example) how will you inform individuals about the study?* | | | | | | | | |
| How will you help support the rights of the data subjects/ research participants? | | | | *As standard PIS documents contain details about how participants can exercise their rights by providing contact details of MMU’s Data Protection Officer. Please confirm this information is included in your PIS, and that you understand that any rights requests from data subjects (right of access/ erasure etc.) must be directed to* [*dataprotection@mmu.ac.uk*](mailto:dataprotection@mmu.ac.uk) *asap.* | | | | | | | | |
|  | | | |  | | | | | | | | |
| 1. **Identify and assess risks** | | | | | | | | | | | | |
| **Describe the source of risk and nature of the potential impact on individuals. Concentrate on potential risks to privacy.** | | | | **Likelihood of harm** | | **Severity of harm** | | | | **Overall risk** | | |
| 1) | *- Is it possible that personal data could be stolen or lost at any point? Are you carrying interview notes or recordings on your person as you travel between locations?*  *- Are you sharing personal data with other parties? Is there a risk it could be compromised?*  *-Are you doing anything with the personal data you collect that the participants may not be aware of, or may not expect?*  *-Are you using a secondary data set and are not able to provide participant information to the individuals?*  *-Is the research so specific and research population so unique that it will be difficult to fully anonymise the results or direct quotes (e.g. does it relate to a rare illness, or unique set of circumstances).* | | | Remote / Possible/ Probable | | Minimal / Significant / Severe | | | | Low / Medium / High | | |
| 2) |  | | |  | |  | | | |  | | |
| 3) |  | | |  | |  | | | |  | | |
| 4) |  | | |  | |  | | | |  | | |
|  |  | | |  | |  | | | |  | | |
| 1. **Identify measures to reduce risk** | | | | | | | | | | | | |
| Identify additional measures you could take to reduce or eliminate the risks identified in step 5 | | | | | | | | | | | | |
| **Risk Number** | | **Options to reduce or eliminate risk** | | **Effect on risk** | | **Residual risk** | | | | **Measure approved?** | | |
| 1) | | *For example:*  *Are you able to reduce the risk by pseudonymising or anonymizing personal data, by encrypting data at rest or in transfer (please note, if using the Research Data Storage solution (RDS), or Dropbox for Business, data is automatically encrypted), using low numbers of research participants, or ensuring that there are restricted access controls in place for any data containing personal data? If participant information cannot be provided directly to participants, could you provide it by some other means such as through general publication?* | | Eliminated / Reduced / Accepted | | Low / Medium / High  Please note:  If the highest residual risk is ‘low’, follow sign off A) below.  If any residual risks are medium or high, instead follow sign off B) below. | | | | Yes / No | | |
| 2) | |  | |  | |  | | | |  | | |
| 3) | |  | |  | |  | | | |  | | |
| 4) | |  | |  | |  | | | |  | | |
|  | |  | |  | |  | | | |  | | |
| 1. **Sign off** | | | | | | | | | | | | |
| **Item** | | | **Name / role/ date** | **Comments/ Advice** | | | | | | | | |
| Data Protection Subject Matter Expert (SME) advice: | | |  |  | | | | | | | | |
| 1. Where residual risk from table 6 is ‘**low**’: **Faculty Head of Research Ethics & Governance** (or their deputy) sign here | | |  |  | | | | | | | | |
| 1. Where residual risk from table 6 is ‘**medium**’ or ‘**high**’: **Faculty PVC sign here (or Director of RKE for NHS applications)** | | |  |  | | | | | | | | |
| Data Protection and Research SME advice accepted or overruled by | | | *Name of Principal Investigator/ Lead Researcher/ Faculty PVC (medium and high risk only)* |  | | | | | | | | |
| **Researcher Sign-off**  **By signing this assessment you are confirming that all details included in the form have been completed accurately and truthfully. You are also confirming that you will comply with all relevant UK data protection laws, and that that research data generated by the project will be securely archived in line with requirements specified in the University’s Retention and Disposal schedule, unless specific legal, contractual, ethical or regulatory requirements apply.** | | | | | | | | | | | | |
| **Name:** | | | | | **Date:** | | | | | | | |
|  | | | | |  | | | | | | | |
| **Please send completed forms to:** [**dataprotection@mmu.ac.uk**](mailto:dataprotection@mmu.ac.uk) | | | | | | | | | | | | |

1. Personal data is anything than can be used to identify a living individual, directly or indirectly. Pseudonymised data is still personal data. If your study uses secondary data that has been collected as part of a previous research exercise, or relies on data gathered from other public sources such as social media or published or non-published material and that data includes personal data, you should still complete this form. [↑](#footnote-ref-1)
2. Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data or data concerning health, sex life or sexual orientation. If your study is likely to lead to special categories of data being collected on a large scale, please tick this statement. For example, your study may not ask specific questions about medical background, but due to the topic, it is likely to be discussed in focus groups or interviews (e.g. a study involving perceptions of accessibility to public buildings is likely to lead to participants discussing background to their personal accessibility requirements and medical history). [↑](#footnote-ref-2)