**DATA PROTECTION IMPACT ASSESSMENT (DPIA) SCREENING QUESTIONS FOR ACADEMIC RESEARCH PROJECTS – Questions relate to the use of personal data**

|  |  |
| --- | --- |
| **Name of Project** |  |
| **Brief Description of Project** |  |
| **Name of PI or PGR student** |  |

When answering these screening questions you need to consider the entire timeline of the project – from the point of collecting or recording personal data, to the end of the project, any dissemination or outputs, longer term archiving and further use.

Data protection duties apply to all our processing of personal data which includes:

* Collection and recording
* Storage, archiving, structuring and organisation
* Use, consultation, retrieval, alteration, alignment and combination, processes of psudonymising and anonymising personal data
* Sharing, disclosure, dissemination
* Deletion, erasure, destruction.

**Screening Questions: Will the processing activities or project involve any of the following?**

|  |  |
| --- | --- |
| **Questions/Criteria** | **Responses** |
| **1** | **A systematic and extensive evaluation (including profiling) of personal aspects relating to individuals which is** * **based on automated processing, and**
* **on which decisions are based that produce legal effects concerning the individual or similarly significantly affect the individual.**

*What does* ***‘systematic and extensive’*** *mean?**The UK GDPR does not define ‘systematic’ or ‘systematic and extensive’ but related guidance states that ‘systematic’ means that the processing:** *occurs according to a system;*
* *is pre-arranged, organised or methodical;*
* *takes place as part of a general plan for data collection; or*
* *is carried out as part of a strategy.*

*The term ‘extensive’ implies that the processing also covers a large area, involves a wide range of data or affects a large number of individuals**What do* ***‘automated processing’*** *or* ***‘automated decision-making’*** *mean?**This is processing or decision making that is not checked by a human being or where there is no manual intervention, e.g. using pre-programmed algorithms and criteria.**What does ‘significantly affect’ mean?** *It is something that has a noticeable impact on an individual and can significantly affect their circumstances, behaviour or choices.*
* *A legal effect is something that affects a person’s legal status or legal rights.*
* *A similarly significant effect might include something that affects a person’s financial status, health, reputation, access to services or other economic or social opportunities. This might include exclusion or discrimination.*
* *Decisions that have little impact generally could still significantly affect more vulnerable people, such as children.*
 | **Yes** [ ]  **No** [ ]  |
| **2** | **Using special category data or criminal offence/conviction data on a large scale***What is* ***‘special category personal data’****?**The UK GDPR defines special category data as:** *personal data revealing****racial or ethnic origin****;****political opinions****;* ***religious or philosophical beliefs****;* ***trade union membership****;*
* ***genetic data****;*
* ***biometric data****(where used for identification purposes);*
* *data concerning****health****;*
* *data concerning a person’s****sex life****;* ***sexual orientation****.*

*Special category data includes personal data****revealing or concerning****the above types of data. Therefore, if you have inferred or guessed details about someone which fall into one of the above categories, this data may count as special category data. It depends on how certain that inference is, and whether you are deliberately drawing that inference.**What does* ***‘criminal offence data’*** *mean?** *This covers a wide range of information about offenders or suspected offenders in the context of criminal activity; allegations; investigations; proceedings; unproven allegations; and even information relating to the absence of convictions.*
* *It also covers a wide range of related security measures, including personal data about penalties; conditions or restrictions placed on an individual as part of the criminal justice process; or civil measures which may lead to a criminal penalty if not adhered to.*
* *It does not cover information about other individuals, including victims and witnesses of crime. However, information about victims and witnesses is likely to be sensitive – see Questions 4, 5, and 8 below.*

*What does* ***‘large scale’*** *mean?* *The UK GDPR does not contain a definition of large-scale processing, but to decide whether processing is on a large scale the ICO advises that we should consider:** *the number of individuals concerned;*
* *the volume of data;*
* *the variety of data;*
* *the duration of the processing; and*
* *the geographical extent of the processing.*

*Examples of large-scale processing include:** *a hospital (but not an individual doctor) processing patient data;*
* *tracking individuals using a city’s public transport system;*
* *an insurance company or bank processing customer data; or*
* *a search engine processing data for behavioural advertising.*

*For other University processing we consider whether the processing covers a significant proportion of a given population, e.g. most students, all staff, a whole cohort.* *For research purposes we recommend that you certainly consider whether studies involving over 1000 participants are ‘large scale’ but depending on the volume of data and variety of data involved this number may be smaller or bigger. You should consider what would be considered ‘large scale’ within your subject area. Funding bodies may also have a definition or view.***Processing of special category personal data or criminal offence data that is NOT on a ‘large scale’ should be considered at Question 8 below.** | **Yes** [ ]  **No** [ ]  |
| **3** | **Systematic or extensive monitoring of individuals OR of a publicly accessible place***What does* ***‘systematic and extensive’*** *mean?**The UK GDPR does not define ‘systematic’ or ‘systematic and extensive’ but related guidance states that ‘systematic’ means that the processing:** *occurs according to a system;*
* *is pre-arranged, organised or methodical;*
* *takes place as part of a general plan for data collection; or*
* *is carried out as part of a strategy.*

*The term* ***‘extensive’*** *implies that the processing also covers a large area, involves a wide range of data or affects a large number of individuals.* | **Yes** [ ]  **No** [ ]  |
| **4** | **Processing personal data about children or other vulnerable individuals***What does* ***‘vulnerable individual’*** *mean?** *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.*
* *Most obviously, children are regarded as vulnerable to the processing of their personal data since they may be less able to understand how their data is being used, anticipate how this might affect them, and protect themselves against any unwanted consequences. This can also be true of other vulnerable sections of the population such as elderly people, patients, asylum seekers, or those with certain disabilities (see Code of Practice for Researchers Working with Vulnerable Populations* [Guidance | Sheffield Hallam University (shu.ac.uk)](https://www.shu.ac.uk/research/excellence/ethics-and-integrity/guidance))*.*
* *An individual or group may also be considered vulnerable if there is an imbalance of power in their relationship with you as this can cause vulnerability for data protection purposes if they believe that they will be disadvantaged if the processing doesn’t go ahead. Employees could be considered vulnerable data subjects where a power imbalance means they cannot easily consent or object to the processing of their data by an employer. This type of vulnerability could also arise due to an individual’s financial situation (e.g. credit rating) or the specific context of the processing (e.g. patients receiving medical care).*
 | **Yes** [ ]  **No** [ ]  |
| **5** | **Processing where a personal data breach could jeopardise the physical health or safety of individuals** | **Yes** [ ]  **No** [ ]  |
| **6** | **Using innovative technologies or the new application of existing technologies to process personal data – including Artificial Intelligence***What does ‘innovative technologies’ mean?**This concerns new developments in technological knowledge in the world at large, rather than technology that is new to you. Using such technology can involve novel forms of data collection and use, possibly with a high risk to individuals’ rights and freedoms. The personal and social consequences of deploying a new technology may be unknown, and a DPIA can help to understand and control such risks.**The ICO gives the following examples of processing using innovative technology:** *artificial intelligence, machine learning and deep learning, algorithms;*
* *connected and autonomous vehicles;*
* *intelligent transport systems;*
* *smart technologies (including wearables);*
* *market research involving neuro-measurement (e.g. emotional response analysis and brain activity);*
* *some ‘internet of things’ applications, depending on the specific circumstances of the processing.*

*It is not just cutting-edge technology that might be classed as innovative. A DPIA may be helpful where implementing existing technology in a new way e.g. a project to design and deploy a large-scale database system that processes customer details.* | **Yes** [ ]  **No** [ ]  |
| **7** | **Processing biometric data (including fingerprint and facial recognition data) or genetic data** | **Yes** [ ]  **No** [ ]  |
| **8** | **Processing of sensitive data (not on a large scale) or data of a highly personal nature i.e. special category personal data, criminal offence data, and other data that individuals would regard as particularly sensitive***What is* ***‘special category personal data’****?**The UK GDPR defines special category data as:** *personal data revealing****racial or ethnic origin****;****political opinions****;* ***religious or philosophical beliefs****;* ***trade union membership****;*
* ***genetic data****;*
* ***biometric data****(where used for identification purposes);*
* *data concerning****health****;*
* *data concerning a person’s****sex life****; s****exual orientation****.*

*Special category data includes personal data****revealing or concerning****the above types of data. Therefore, if you have inferred or guessed details about someone which fall into one of the above categories, this data may count as special category data. It depends on how certain that inference is, and whether you are deliberately drawing that inference.**What does* ***‘criminal offence data’*** *mean?** *This covers a wide range of information about offenders or suspected offenders in the context of criminal activity; allegations; investigations; proceedings; unproven allegations; and even information relating to the absence of convictions.*
* *It also covers a wide range of related security measures, including personal data about penalties; conditions or restrictions placed on an individual as part of the criminal justice process; or civil measures which may lead to a criminal penalty if not adhered to.*
* *It does not cover information about other individuals, including victims and witnesses of crime. However, information about victims and witnesses is likely to be sensitive – see Questions 4, 5, and 8 below.*

***In addition*** *to special category personal data and criminal offence data, there are other types of personal data that may be considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject’s daily life (such as financial data that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications.***Processing of special category personal data or criminal offence data on a large scale is covered in Question 2 above.** | **Yes** [ ]  **No** [ ]  |
| **9** | **Invisible or covert processing: Collecting personal data without providing a privacy notice/participant information sheet to the individual OR collecting new personal data from a 3rd party source (not the individual)***What does* ***‘invisible processing’*** *mean?** *Where we are unable to provide a participant information sheet/privacy notice to a data subject, any data processing results in a risk to the individual’s interests as they cannot exercise any control over our use of their data. In particular, they are unable to use their data protection rights if they are unaware of the processing. This is true even if the processing itself is unlikely to have any negative effect.*
* *There is also a risk of breaching the fairness and transparency requirements if the processing, or any outcome from it, may not be reasonably foreseen by the individual.*
* *For these reasons, processing in this way is only permitted by the UK GDPR in limited circumstances. These include where to provide the privacy information proves****impossible****or would involve a****disproportionate effort****.*
* *Circumstances when it is impossible to provide privacy will only arise rarely, for example where you have no contact details for individuals and have no reasonable means of obtaining them.*
* *A DPIA will help assess and demonstrate whether the approach is proportionate, how best to mitigate the impact on individuals’ ability to exercise control over their data, and whether other measures can be put into place to support the exercise of their rights. It will also help to demonstrate how the processing complies with fairness and transparency requirements.*
* Where researchers are obtaining datasets from another organisations, the information provided to the data subjects by that organisation should also be considered.
 | **Yes** [ ]  **No** [ ]  |
| **10** | **Tracking an individual’s geolocation or behaviour, including online behaviour** | **Yes** [ ]  **No** [ ]  |
| **11** | **Large scale processing of personal data** *What does* ***‘large scale’*** *mean?* *The UK GDPR does not contain a definition of large-scale processing, but to decide whether processing is on a large scale the ICO advises that we should consider:** *the number of individuals concerned;*
* *the volume of data;*
* *the variety of data;*
* *the duration of the processing; and*
* *the geographical extent of the processing.*

*Examples of large-scale processing include:** *a hospital (but not an individual doctor) processing patient data;*
* *tracking individuals using a city’s public transport system;*
* *an insurance company or bank processing customer data; or*
* *a search engine processing data for behavioural advertising.*

*For other University processing we consider whether the processing covers a significant proportion of a given population, e.g. most students, all staff, a whole cohort.* *For research purposes we recommend that you certainly consider whether studies involving over 1000 participants are ‘large scale’ but depending on the volume of data and variety of data involved this number may be smaller or bigger. You should consider what would be considered ‘large scale’ within your subject area. Funding bodies may also have a definition or view.* | **Yes** [ ]  **No** [ ]  |
| **12** | **Denial of Service: The processing itself will/could prevent data subjects from exercising a right, using a service, entering into a contract, or accessing an opportunity or benefit** | **Yes** [ ]  **No** [ ]  |

**For a DPIA, we would normally also ask the following question. As this is a routine research activity, this does not automatically lead to a risk to data subjects, however, if you think that there are additional risks to data subjects based on this kind of processing please answer YES.**

|  |  |  |
| --- | --- | --- |
| **13** | **Are there risks from matching, combining, or comparing datasets processed for different purposes or from different sources?*****When might this pose a risk to data subjects?**** *Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers may exceed the reasonable expectations of the data subject;*
* *Terms, definitions, and fields in different datasets may not match exactly, producing incorrect analyses and/or inaccurate data.*
 | **Yes** [ ]  **No** [ ]  |

|  |
| --- |
| **Screening outcome**  |
|  | **Will the processing involve ANY of the activities in questions 1 – 5?**  | **Yes** [ ]  **No** [ ]  **If YES, DPIA required**  |
|  | **Will the processing involve TWO OR MORE of the activities in questions 6 – 12?** | **Yes** [ ]  **No** [ ]  **If YES, DPIA required** |
|  | **Will the processing involve ONE of the activities in questions 6 – 12?** | **Yes** [ ]  **No** [ ]  **If YES, DPIA not usually required but may be helpful in protecting the interests of the data subjects– PI to determine.** |
|  | **Will the processing involve the activity in question 13 in a way that will be likely to pose a risk to individuals?** | **Yes** [ ]  **No** [ ]  **If YES, DPIA required** |
|  | **Will the processing involve NONE of the activities 1-13?** | **Yes** [ ]  **No** [ ]  **If YES, DPIA not required** |
|  | **Based on the above criteria, is a DPIA required for the proposed project / activity?** | **DPIA REQUIRED** [ ] **DPIA NOT REQUIRED** [ ] **DPIA NOT REQUIRED BUT PI HAS CHOSEN TO UNDERTAKE** [ ]  |

**You can decide to conduct a DPIA if you would find this helpful even where the screening questions do not indicate a requirement. Some funding bodies may require a DPIA.**

**If you are not sure whether a DPIA is required or would like further information, please contact the Information Governance Team:** **DPO@shu.ac.uk****.**

|  |
| --- |
| **Further advice from DPO (if sought):** |
| **Further input from funder (if sought):** |

**DPIA FOR ACADEMIC RESEARCH PROJECTS**

* **To be completed if the screening questions confirm a requirement, or where a PI (or Director of Studies) determines a DPIA to be helpful.**
* It may be appropriate to copy some information from the research proposal or ethics application/approval, but please remember that a DPIA focuses on the use of personal data, the impact of processing on data subjects, and risks to data subjects.
* **Please note that if a full DPIA is required, no personal data should be processed until DPIA has been completed and signed off.**
* Further advise and support is available from the Information Governance Team / DPO (dpo@shu.ac.uk).

|  |  |  |
| --- | --- | --- |
| **Requirements** | **PI/Project Manager Response** | **DPO/IG Team Comments** |
| **STEP 1 - Describe the purposes, personal data, and processing** |
| **Describe the nature of the processing:** * How will you collect, use, store and delete data?
* What data security measures are you implementing?
* What is the source of the data?
* Will you be sharing data with anyone?
* You might find it useful to refer to a flow diagram or other way of describing data flows.
 |  |  |
| **Describe the scope of the processing:** * What is the nature of the data?
* What categories of personal data will be collected and/or used?
* Describe any special category or criminal offence data.
* How much data will you be collecting and using?
* How often?
* How long will you keep it?
* Who are the data subjects?
* How many individuals are affected?
* What geographical area does it cover?
 |  |  |
| **Describe the context of the processing:** * What is the nature of your relationship with the individuals?
* How much control will they have?
* Would they expect you to use their data in this way?
* Describe any processing relating to children or other vulnerable groups, including instances where there may be an imbalance of power in the relationship with the data subjects.
* Are there prior concerns over this type of processing or security flaws?
* Are there any novel elements of the processing that could impact on data subjects? E.g. could the processing be misunderstood by or have an unintended impact on the data subjects?
* Is the technology that is being used fully developed and understood? Are there any concerns about the potential impact on data subjects from the use of the technology?
* Are there any current issues of public concern that you should factor in?
* Are you signed up to any approved code of conduct or certification schemes, sector codes of practices?
* Are there any other relevant laws or regulations that need to be taken into consideration?
 |  |  |
| **Describe the purposes of the processing:** * What do you want to achieve?
* What are the benefits of the processing?
* Who will benefit? Is there a clear public interest/benefit to the processing?
 |  |  |
| **STEP 2 – DETAIL ANY RELEVANT ConsultationS OR PATIENT AND PUBLIC INVOLVEMENT** |
| * Have you sought the views of any individuals who will be involved in or impacted by the project (or their representatives? Focus groups, pilot studies, Patient and Public Involvement (PPI) would be examples.
* Have you consulted with any partners, stakeholders, other researchers, or experts on any aspect of the data processing for this project, in particular on what the impact on data subjects is likely to be from the research?
* Have you made any other assessments of the potential concerns that data subjects might have? E.g. drawn on experience from previous studies?
* If you have consulted or have undertaken PPI, what concerns or impacts were raised in relation to the processing of personal data, if any, and how have you addressed these?
* Have you submitted an ethics application?
* Have you received ethics approval?
 |  |  |
| **STEP 3 - Assess COMPLIANCE, necessity and proportionality** |
| **Describe compliance and proportionality measures, in particular:** * Does the processing actually achieve your purpose?
* Is there another way to achieve the same outcome?
* Can you achieve the same purpose by processing less data, or by processing the data in a less intrusive way?
* How will you ensure data quality and data minimisation?
* What information will you give individuals?
* How will you help to support their rights? (e.g. right of access, right to erasure)
 |  |  |
| **The lawful basis for processing personal data for research purposes at the University is usually public task/public interest because the University has statutory powers to conduct research:***“processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”.*This would work alongside ethical consent for an individual to participate in a study.* Is this correct for this project?
* If not, are you relying on a data protection lawful basis of legitimate interests or the consent of each participant? You should set out the reasons for a different lawful basis.
 | [ ]  Yes – public task/public interest[ ]  No – Legitimate interests [ ]  No – Consent of each participant Reasons for Legitimate interests or UK GDPR consent: |  |
| **Are there any partners who will have access to the personal data?** * **If yes**, please list the companies/organisations.
* Are any of the partners located outside the UK?
* If so, where?
* **If yes**, you will be likely to require a data sharing agreement or data protection clauses within your partnership/collaboration agreement or contract. Contact: ! RIS Legal Services - RIS-LegalServices@shu.ac.uk
 | [ ]  No[ ]  YesLead partner:Other partners:Partners outside the UK, including location/country: |  |
| **Will any personal data be shared with a funding body for this project?*** **If yes**, you will be likely to require a data sharing agreement or data protection clauses within the funding agreement or contract. Contact: ! RIS Legal Services - RIS-LegalServices@shu.ac.uk
 | [ ]  No[ ]  YesFunder: |  |
| **Are there any sub-contractors/suppliers/organisations acting as data processors who will have access to the personal data?*** **If, yes** please list the companies/organisations.
* **If yes**, supplier checks and a data processing agreement or data protection clauses within the supplier contract will normally be required. Please confirm that where required, checks/due diligence processes and a data processing agreement are in place or will be put in place prior to any data processing. <https://sheffieldhallam.sharepoint.com/sites/3037/SitePages/Bids-and-Tenders.aspx>
* Are any of the sub-contractors/suppliers/data processors located outside the UK?
* If so, where?
 | [ ]  No [ ]  Yes – transcription services[ ]  Yes – other data processor within UKList UK data processors:[ ]  Yes – data processor outside UKList non-UK data processors, including location/country: |  |

**STEP 4 - ASSESSING RISK AND IMPACT ON DATA SUBJECTS**

**The risk assessment should focus on the risk to data subjects, not to the University or to another organisation.**

**Please see example risks, impacts, and actions below (after risk table).**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **#** | **1. Risk** | **2. Describe the source of the risk or the threat/weakness that may lead to the risk occurring.**  | **3. What is the potential impact on individuals****(See examples below this table)** | **4. Likelihood of harm:** | **5. Severity of harm:** | **6. Overall risk:** | **7. Actions to eliminate or reduce risk****(See examples below this table)****Have you reduced the likelihood and/or severity of harm to the data subject(s)?** | **8.Overall residual risk** |
|  |  |  |  | [ ]  Rare[ ]  Unlikely[ ]  Possible[ ]  Likely[ ]  Almost Certain  | [ ]  Negligible[ ]  Minor[ ]  Moderate[ ]  Serious[ ]  Catastrophic  | [ ]  Low[ ]  Medium[ ]  High |  | [ ]  Low[ ]  Medium[ ]  High |
|  |  |  |  | [ ]  Rare[ ]  Unlikely[ ]  Possible[ ]  Likely[ ]  Almost Certain | [ ]  Negligible[ ]  Minor[ ]  Moderate[ ]  Serious[ ]  Catastrophic  | [ ]  Low[ ]  Medium[ ]  High |  | [ ]  Low[ ]  Medium[ ]  High |
|  |  |  |  | [ ]  Rare[ ]  Unlikely[ ]  Possible[ ]  Likely[ ]  Almost Certain | [ ]  Negligible[ ]  Minor[ ]  Moderate[ ]  Serious[ ]  Catastrophic  | [ ]  Low[ ]  Medium[ ]  High |  | [ ]  Low[ ]  Medium[ ]  High |
|  |  |  |  | [ ]  Rare[ ]  Unlikely[ ]  Possible[ ]  Likely[ ]  Almost Certain | [ ]  Negligible[ ]  Minor[ ]  Moderate[ ]  Serious[ ]  Catastrophic  | [ ]  Low[ ]  Medium[ ]  High |  | [ ]  Low[ ]  Medium[ ]  High |
|  |  |  |  | [ ]  Rare[ ]  Unlikely[ ]  Possible[ ]  Likely[ ]  Almost Certain | [ ]  Negligible[ ]  Minor[ ]  Moderate[ ]  Serious[ ]  Catastrophic  | [ ]  Low[ ]  Medium[ ]  High |  | [ ]  Low[ ]  Medium[ ]  High |

**Examples of risks (column 1):**

|  |  |
| --- | --- |
| Data is processed for unspecified/unlawful purposes/not within expectations of data subjects  | Data is not anonymised when it should/can be and/or is not properly anonymised. |
| Excessive data is processed | Re-identification of pseudonymised data by data processor or third party |
| Insufficient data is collected/processed – data is not adequate for the purpose | Data may not be accurate (e.g. obtained from an unverified or old list) |
| Data is not kept up to date | Risk to accuracy of data due to matching/combining data from different sources |
| Data is kept for longer than is necessary by the University/processor | Unauthorised destruction or loss of data |
| Data is shared too widely within the University | Data processor fails to process data in accordance with our instructions |
| Data is shared unlawfully or inappropriately outside the University | Personal data of children processed without appropriate safeguards/parental authority |
| Data stolen or modified in transit | Consent of data subject is not received and/or the University is unable to demonstrate consent |
| Data stolen or modified at rest in our premises/in our systems | Consent of data subject not freely given (for example employer/employee processing) |
| Data stolen or modified at rest in data processor premises/in data processor systems | The data subject is particularly vulnerable or there is a potential imbalance of power between the individual and the data controller |
| Data transferred overseas to a jurisdiction that does not adequately protect data subject rights | Data is processed in contravention of data subject rights and/or Data subjects unable to exercise their rights |
| Unauthorised access to personal data | Unwanted modification of personal data |

**Examples of Potential Impact / Damage to Individuals (column 3):**

|  |  |  |  |
| --- | --- | --- | --- |
| risk of physical harm | loss of control over personal data | limitation/deprivation of their rights | discrimination |
| identity theft or fraud | damage to reputation  | (significant) social disadvantage | inability to access data or services |
| financial loss / other economic impact | loss of confidence in the University (or other party) | loss of time due to effort required to resolve issue | psychological distress / anxiety |
| identification through unauthorised reversal of pseudonymisation | loss of confidentiality of personal data protected by professional secrecy |  |  |

**Examples of actions that could be implemented which would reduce the identified risks (column 7) - this is not an exhaustive list and will require additional detail, please include any other actions that may help reduce or avoid the risks.**

|  |  |  |  |
| --- | --- | --- | --- |
| Not collecting certain types of data | Reducing the scope of the processing | Short retention periods or reducing data retention periods | Training staff to understand and manage the risks (e.g. SHU GDPR module, training from IG Team, or other training) |
| Additional technological security measures | Anonymising data  | Preparing/updating internal guidance & procedures | Using a different technology |
| Physical security of offices/buildings | Pseudonymising data | Restricting access and managing access | Prohibit use of private devices/BYOD |
| Implementing data-sharing agreements | Making changes to privacy notices/participant information sheets | Enabling individuals to opt-out  | Help individuals to exercise their rights |
| Clear roles and responsibilities, procedures, and policies | Providing privacy notices/participant information in different formats or languages | Managing staff leavers and movers | Spot checks and audits |
| Encryption of data, e.g. encrypted emails, encrypted mobile devices | Secure storage of paper documents and mobile devices/equipment used to process personal data | Secure disposal of paper documents and equipment used to process personal data | Managing suppliers/data processors |

**DATA PROCESSING IMPACT ASSESSMENT – PROCESS LOG**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Responsibility** | **Name/Signature** | **Date** | **Decisions** | **Record of decision / notes** |
|  | **SCREENING QUESTIONNAIRE TO BE COMPLETED FOR ANY NEW PROJECT, PLAN, ACTIVITY THAT INVOLVES PROCESSING PERSONAL DATA** |
| 1 | Screening questionnaire completed  | Principal Investigator/Project Manager/ Postgraduate Research Student |  |  |   |  |
|  | **DATA PROTECTION IMPACT ASSESSMENT PROCESS** |
| 2 | DPIA Form completed  | Principal Investigator/Project Manager/Postgraduate Research Student |  |  |  |  |  |
| 3 | Advisory/risk assessment (IG team will advise if the DPIA should be reviewed by other teams) | IG Team/DPO |  |  |  |  |  |
| Other , e.g. IT Security Team |  |  | Consultation required? | Y/N |  |
| 4 | ICO consultation (only required if residual risks are high risk) | DPO |  |  | Consultation required? | Y/N |  |
| 5 | DPIA updated if necessary and finalised by PI. Postgraduate Research Students should obtain approval from their Director of Studies. | Principal InvestigatorPostgraduate Research Student (and Director of Studies) |  |  |  |  |  |
| 6 | Final version sent to IG Team/DPO DPO@shu.ac.ukand retained in the PI’s/PGR student’s project file | IG Team/DPO and PI/PGR student |  |  |  |  |  |
| 7 | PI/PGR student approval for completed DPIA to be shared internally by IG team as an example for other researchers.The PI/PGR student should also consider whether to publish the DPIA externally if required for the benefit of the research project. | Principal Investigator/PGR student |  |  | [ ]  7a Yes, DPIA can be shared internally as example for other researchers.[ ]  7a No, access to DPIA needs to be restricted – cannot be shared internally |  |
| 8 | Periodic/ongoing review | Principal Investigator/Project Manager/PGR student |  |  |  |  | A DPIA is a ‘live’ document and should be reviewed regularly AND updated if there is any change to the processing of personal data considered between scheduled reviews. If a DPIA is required, please complete the version control record below each time it is reviewed. Major changes should be discussed with the Information Governance team. Updated DPIAs must be sent to the Information Governance team (dpo@shu.ac.uk) |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Summary of changes/updates** | **Date** | **Date of next scheduled review**  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |