Robert Gordon University – Privacy Impact Assessment Guidance

A Privacy Impact Assessment (PIA) is a process which helps assess privacy risks to individuals in the processing of personal data. A failure to embed privacy protective measures may result in a breach of data protection law, along with potential declaration of incompatibility with the Human Rights Act or prohibitive costs in retro-fitting a system to ensure legal compliance or address concerns about privacy.

The PIA template is a practical and effective tool to identify and address any data protection and privacy concerns at an early stage, building compliance in from the outset. A PIA should be carried out whenever there is a change that is likely to involve a new use or significantly change the way in which personal data is processed, for example when a replacement system for an existing database is being implemented.

A PIA should **not** be considered to be as a one-time activity that when completed should not again be considered. It is intended to be incorporated in to the life cycle of a project, task or activity, ensuring that data protection is designed into the University processes. Therefore as a project, task or activity evolves it may be necessary to carry out multiple PIA's or to refer back to the initial PIA and reconsider the findings.

Any systems that do not identify individuals in any way do not require a PIA to be performed. However, you should carefully consider how "anonymous" data is, if it could in fact be identifiable when combined when other information.

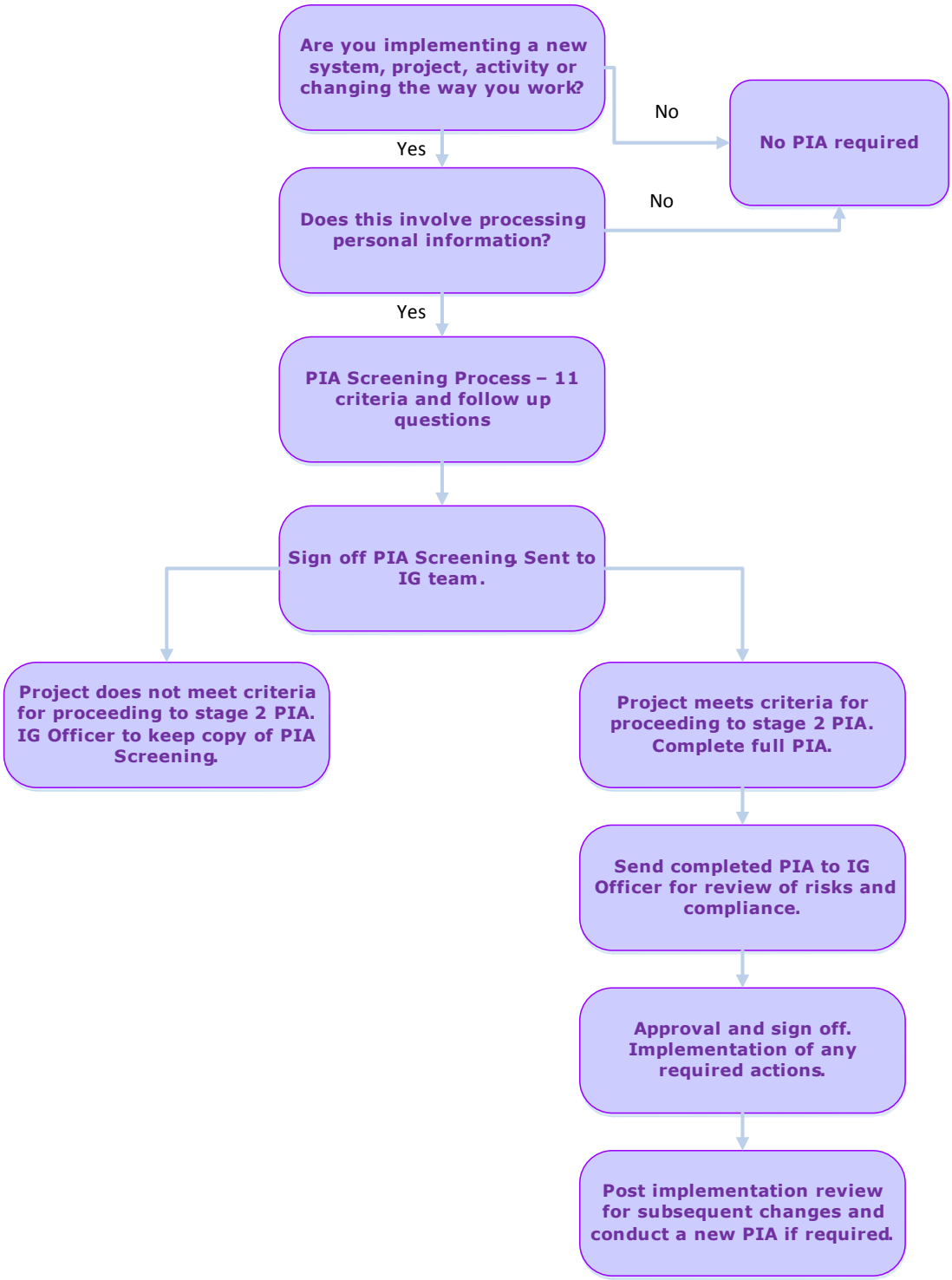
There is a requirement under the GDPR, when you are undertaking an activity that will involve processing personal data e.g. "any information relating to an identified or identifiable natural person" to carry out a PIA screening exercise, which then may result in a full PIA. Therefore any instance of undertaking a new or changed activity in processing personal data **must** go through a PIA screening exercise.

The Information Governance officer can advise on the completion of a PIA, further to the information presented within this guide.

Who is responsible for completing a PIA?
Any person who is responsible for introducing new or revised services, projects or activities should complete the PIA process. The Information Governance officer should be consulted throughout the

process. If the personal information is processed by any IT system then the Director of IT must be consulted.

PIA Flowchart



Two Stages of a PIA

Stage 1 – The Screening Questions
This section is to be completed by the project lead or individual responsible for delivering the proposed change.

The purpose of the screening questions is to assess whether a full PIA is required and to ensure that the investment is proportionate to the risks involved. Completed screening questions should be returned to the Information Governance Officer and either of the following will occur:

1. The screening process has not identified any PIA concerns and the process is complete
2. If you have answered 'yes' to any of criteria 1-4 you must proceed to a full PIA. If you have answered 'yes' to two or more of criteria 5–11 then you should also proceed to a full PIA.

Meeting the conditions as described at point 2 above may mean that there is a potential risk factor that will have to be further analysed to ensure the risks are identified, evaluated and fully mitigated. It is therefore necessary to conduct a full impact assessment in order to address this.

Stage 2 – Privacy Impact Assessment

The responses to the screening questions will have given an indication if this is required. This should be completed by the project lead or individual responsible for delivery of the proposed change, however it should be signed off by the Head of Department/School and may require sign-off from the Head of IT and the Information Governance officer as well, depending on the level of risks identified.

A full PIA has 8 steps involved in the process. Vital to this process is the need to consider the GDPR principles throughout. Please refer to annex 1 which lays out the principles and the key questions to consider in regards to these.

Step One – Identify the need for a PIA

At this stage you should detail what criteria were met to require the assessment and also fully explain the aim of the activity and what the benefits of it will be to the organisation, individuals etc. At this point you may want to include links to documents such as a project proposal. Key items to address include:

- Description and summary of activity/task/project
- Purpose and key benefits of activity/task/project
- Implementing Department

- Details of Lead Staff member
- Criteria for carrying out PIA (from screening exercise)
- Key stakeholders
- Implementation Date

Step Two – Describe the Information Flows
At this stage you should fully describe how data will be processed. The below illustrates examples of ways in which personal data may be processed. Please note that this is not an exhaustive list.

- Collecting information via an application form, over the phone or via a website;
- Publishing information;
- Selling information;
- Using information for administration;
- Using information for marketing;
- Intercepting information;
- Recording information;
- Data matching, data mining or profiling;
- Archiving information;
- Reading information from a screen;
- Disclosing or passing information to another organisation or individual
- Shredding information in a personal file or erasing information from electronic media;
- Making information available on a website.

It will likely be useful to include a flow diagram or something similar to make clear the data flows. You should also be clear at this stage how many individuals are going to be included or affected by the activity. Other considerations may be to think about how the information will be stored and if there is a way to audit access to the data.

At this stage you must also detail the type of personal data that will be processed. The below list gives examples of data that may be collected. Please note that collection of "special category" data, as defined below, is prohibited unless certain conditions are met.

- Is this a new or changed use of personal data that is already collected? Is the changed use of the personal data lawful?
- What data will be collected?
    - Forename/Surname
    - Date of Birth
    - Age
    - Gender
    - Address
    - Postcode

    - Other unique identifiers (specify)
    - Any other data (specify)
- Will any data classed "special category" be collected?
    - Racial or ethnic origin
    - Political opinions
    - Religious or philosophical beliefs
    - Trade Union membership
    - Processing of genetic or biometric data for the purpose of uniquely identifying a person
    - Data concerning health
    - Data concerning an individual's sex life or sexual orientation

Step Three: Consultation Requirements

At this stage you should consider privacy risks with particular concern to sharing of personal data. Any sharing of data should be noted in section two in the flow mapping exercise at step two. Questions to consider include:

- Are any other organisations involved in processing the data?
- What is their name and ICO notification number?
- Are they the data controller or data processor[1]?
- Are they compliant with the rules stipulated in procurement contracts?
- Does the work involve employing contractors external to RGU? If yes, reference confidentiality agreement.
- Will the data be shared outside the organisations listed above? Will this be an international transfer? If yes, describe who and why.
- What is the legal basis to share the data?
- What safeguards are in place against onward transmission of the data?

Step Four: Identify the privacy and related risks

There are a wide range of issues to consider under this step. A privacy risk may have been highlighted at step three when considering sharing the data. At this stage you should also evaluate the level of risks identified. If data is to be shared, consider questions such as:

- How will data be transferred? E.g. what method will be used?
- Will personal data be transferred internationally? Further consider the below:

[1] The data controller is the organisation that is processing personal data and has authority to decide how and why it is to be processed. A data processor is an organisation that processes personal data on behalf of another organisation but does not have control over how and why.

    - Will this be within the European Economic Area (EEA)[2]? If yes, this can be transferred within the regulations.
    - Will this be out-with the EEA but within one of the European Commission approved countries as outlined within the ICO guidance[3]? This may be transferred in line with ICO guidelines.
    - Will this be out-with the EEA and not a European Commission approved country? Please refer to ICO guidance[4].
- How will information be kept up to date and checked for accuracy and completeness?
- Who will have access to the information?
- Will any information be sent offsite e.g. out-with the University and its computer network[5].
- How will individuals be informed about the proposed uses of their personal data? You may wish to consider a privacy notice.
- Are arrangements in place for recognising and responding to an individual's subject access request for the personal data being collected?
- Will individuals be asked for consent for their information to be collected and/or shared?
- If not consent, what is the legal basis for collecting the data? What associated risks are there?

Step Five:
At step five you should consider any risks that have been highlighted in step four and solutions to address them such as ways to eliminate or reduce the risks. You should also consider at this stage if a risk is to be accepted moving forward or unacceptable.

Step Six:
Step six follows closely on from step five and asks that if solutions for risks have been identified in step five that you list the approved solution relevant to the respective risks. This should then be approved by an individual with appropriate seniority. This may include where a risk has been identified and cannot be reduced or eliminated but has been deemed acceptable to bear. This will require sign off as relevant to the level of risk but would likely involve the Head of School/Department and the Information Governance Officer.

---

[2] https://www.gov.uk/eu-eea
[3] https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/
[4] https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/
[5]https://you.rgu.ac.uk/org/ig/Documents/MobileComputingPolicy%20Issue%201-0.pdf

Step Seven:
At this final stage you must identify the next steps for implementing the findings of the privacy impact assessment, including steps for implementing solutions identified at section 6. At this stage you should also consider when you will carry out the post implementation review and evaluation. This should be an ongoing process that will assist in monitoring risks and identifying any new risks as the activity evolves.

Step Eight:
At the sign off stage, there are several options to have the Privacy Impact Assessment approved.

- No risk identified – sign off by project lead or equivalent.
- Risk identified and eliminated – Sign off must involve the Head of School or Department.
- Risk identified and reduced – Sign off must involve the Head of School or Department, the Information Governance Officer and may require sign off from the Head of IT and dependent on the level of risk from senior management.
- Risk identified and unable to reduce but deemed acceptable to carry forward. Sign off must be relevant to the level of risk posed but may involve the Head of School or Department, the Information Governance Officer, the Head of IT and senior management.

Annex 1

Linking the PIA to the General Data Protection Regulations principles

The University is subject to the requirements of the GDPR along with other relevant legislation such as the Human Rights Act. The below should be considered during the PIA process to help identify where there is a risk that the project will fail to comply with relevant legislation.

Principle 1
Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

1. Have you identified the purpose of the project?
2. How will you tell individuals about the use of their personal data?
3. Do you need to amend your privacy notices?
4. Have you established which conditions for processing apply?
5. If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
6. Will the systems you are putting place allow you to respond to subject access requests more easily?
7. If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

In regards to the Human Rights Act;

1. Will your actions interfere with the right to privacy under article 8?
2. Have you identified the social need and aims of the project?
3. Are your actions a proportionate response to the social need?

Principle 2
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

1. Does your project plan cover all of the purposes for processing personal data?
2. Does the processing allow for the "right to be forgotten"?
3. Have you identified potential new purposes as the scope of the project expands?

Principle 3
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

1. Is the quality of the information good enough for the purposes it is used?

2. Which personal data could you not use, without compromising the needs of the project?

Principle 4
Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

1. How are you ensuring that personal data obtained from individuals or other organisations is accurate?
2. If you are procuring new software does it allow you to amend data where necessary?
3. How do you ensure the data remains accurate?

Principle 5
Personal data shall be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific of historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

1. What retention periods are suitable for the personal data you will be processing?
2. Does existing software or are you procuring software that will allow you to delete information in line with your retention periods?
3. How have you determined retention periods?

Principle 6
Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

1. What systems are in place to protect against any security risks? Are there any new systems being put in place for this reason?
2. What training and instructions are necessary to ensure that staff know how to treat personal data securely or how to use necessary systems securely?
3. Does the system have any features which would be beneficial in the event of a data breach?

There is a further requirement under Article 5(2) of the GDPR that states that the data controller shall be responsible for, and be able to demonstrate compliance with the principles.

1. Does the processing of personal data conform to University policy and procedures?