University of Northampton

Records Management Office Documentation

Version	Date of Change	Notes	Editor
6.0	15/04/2020	Document Review Minor layout changes	Gareth Reeves
7.0	11/01/2021	Guidance updated to match form	Gareth Reeves

Guidance on completing Privacy Impact Assessments

Contents

Introduction

Why should we bother?

- Such assessments are a legal requirement of the General Data Protection Regulations
- The process will assist the University in identifying and minimising risks to privacy at the start of, and throughout any new project.
- The process identifies potential risks early in the process so that they can be addressed.
- Conducting a PIA benefits the University by aiding shaping better policies and systems to improve relationships between the University and individuals.

What do we mean by privacy?

- Physical privacy – the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information
- Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages

What are the risks to privacy?

- Privacy risks can arise through personal information being:
- Inaccurate, insufficient or out of date;
- Excessive or irrelevant;
- Kept for too long;
- Disclosed to those who the person it is about does not want to have it;
- Used in ways that are unacceptable to or unexpected by the person it is about; or
- Not kept securely

The completion of a PIA should minimise such privacy risks

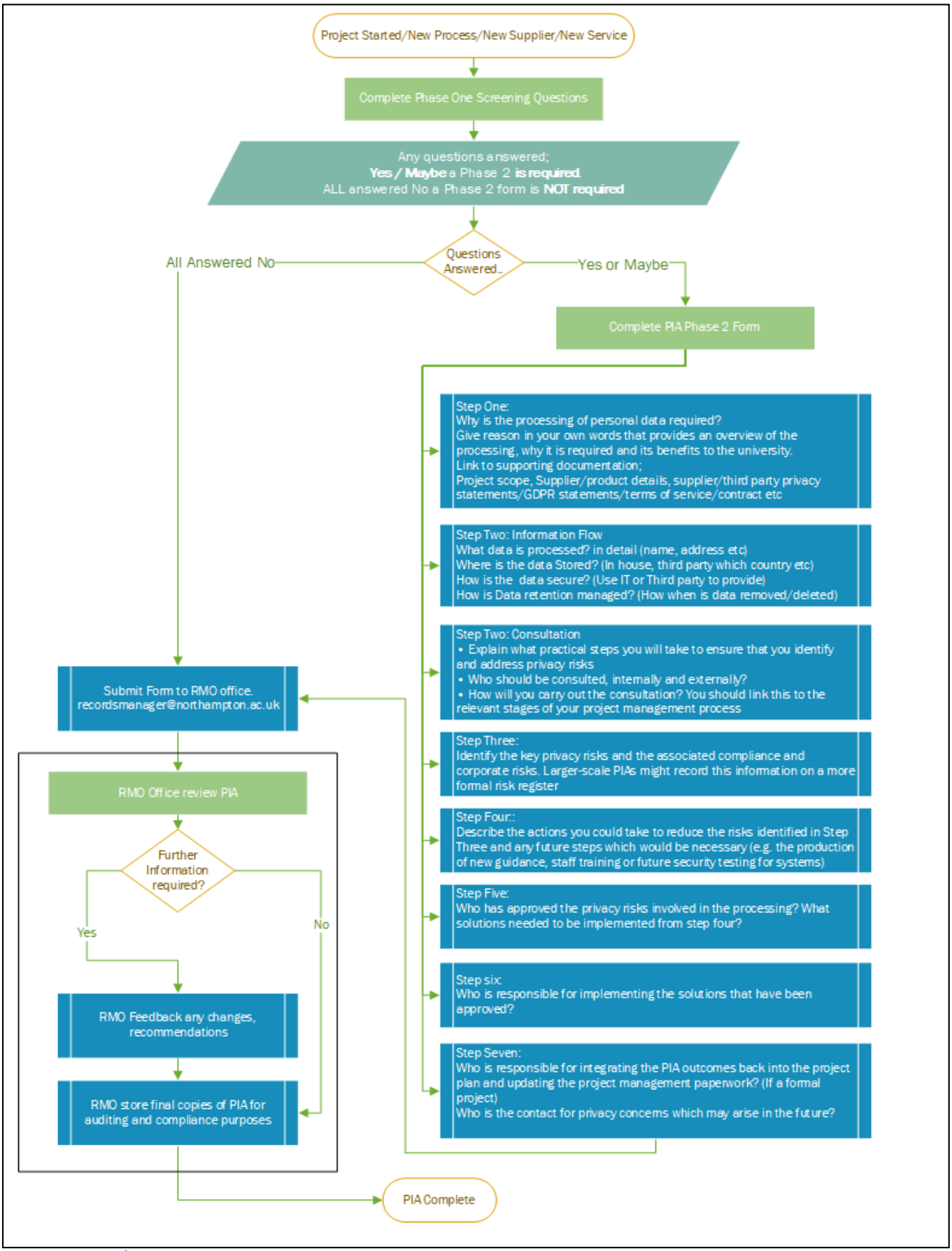
What are the benefits of a PIA?

- Privacy impact assessments (PIAs) are a requirement the University has to comply with in order to meet the standards governed by General Data Protection Regulations (GDPR).
- Carrying out an effective PIA should benefit the people affected by a project and the team carrying out the project.
- It is also a way to evidence to the Information Commissioner's Office that privacy has been carefully and fully considered prior to the collection of any data and to demonstrate that processing complies with GDPR.
- Improves transparency making it easier for individuals to see how their information is being used.
- Consistent use of PIAs will increase the awareness of privacy and data protection issues within the University and ensure that all relevant staff involved in designing projects think about privacy at the early stages of a project.

Introduction to the PIA Process

Key Points:

- The PIA process is a flexible one that can be integrated with existing approaches to managing projects. The time and resources dedicated to a PIA should be scaled to fit the nature of the project or new/updated personal data processing requirement
- A PIA should begin early in the life of a project, but can run alongside the project development process
- PIAs are not limited to project work. PIAs are required for any significant changes to existing processes as well as entirely new processes e.g new supplier for existing process or an entirely new process not previously undertaken by the university.
- A PIA should incorporate the following steps (see diagram on next page)..


Project Started/New Process/New Supplier/New Service
Complete Phase One Screening Questions
Any questions answered;
Yes / Maybe a Phase 2 is required
ALL answered No a Phase 2 form is NOT required
Questions Answered..
All Answered No
Yes or Maybe
Complete PIA Phase 2 Form
Step One:
Why is the processing of personal data required?
Give reason in your own words that provides an overview of the processing, why it is required and its benefits to the university.
Link to supporting documentation;
Project scope, Supplier/product details, supplier/third party privacy statements/GDPR statements/terms of service/contract etc
Step Two: Information Flow
What data is processed? in detail (name, address etc)
Where is the data Stored? (In house, third party which country etc)
How is the data secure? (Use IT or Third party to provide)
How is Data retention managed? (How when is data removed/deleted)
Step Two: Consultation
• Explain what practical steps you will take to ensure that you identify and address privacy risks
• Who should be consulted, internally and externally?
• How will you carry out the consultation? You should link this to the relevant stages of your project management process
Step Three:
Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register
Step Four::
Describe the actions you could take to reduce the risks identified in Step Three and any future steps which would be necessary (e.g. the production of new guidance, staff training or future security testing for systems)
Step Five:
Who has approved the privacy risks involved in the processing? What solutions needed to be implemented from step four?
Step six:
Who is responsible for implementing the solutions that have been approved?
Step Seven:
Who is responsible for integrating the PIA outcomes back into the project plan and updating the project management paperwork? (If a formal project)
Who is the contact for privacy concerns which may arise in the future?
Submit Form to RMO office.
recordsmanager@northampton.ac.uk
RMO Office review PIA
Further Information required?
Yes
No
RMO Feedback any changes, recommendations
RMO store final copies of PIA for auditing and compliance purposes
PIA Complete

Step One: Identify the need for a PIA

This step will describe the business case for the processing and why personal data is being processed. Use the questions that were answered Yes or Maybe from the Screening questions as a starting point.

For Projects, the description can be a link to or a copy of any pre-existing project scope or business case if this covers these points.

When processing does not relate to a project and a PIA is required for (but not limited to);

- New Supplier of third-party software or cloud product (SaaS)
- Renewal of existing software or third-party contract where a PIA has not previously been completed (in place prior to GDPR)

In the cases above, include with the description of the processing any supporting documentation especially where a third-party company/service is being employed, documentation such as;

- Contract
- Terms of Service
- Privacy Notice
- GDPR Statements, if separate from above

The Phase Two form last page contains a table to enter any links to supporting documentation for your convenience.

Providing the supporting documentation is needed to allow the compliance team to perform more in-depth checks if required into the GDPR compliance of the third party and any service. This demonstrates due diligence has been completed if the processing is audited or is subject to a review by the ICO following a complaint.

Step Two: Describing how the information flows

Key Points:

- Check if a data audit already exists for this processing as this can provide a starting point for this section, if an existing process the records management team will have a copy of the audit and can supply a copy on request.
- This process can help to identify potential unforeseen or unintended uses of the data (for example data sharing)
- Potential future uses of the information can be identified at this stage, even if they are not immediately necessary – this enables the consent of the individual to be sought in anticipation

As part of the PIA process organisations should describe how information is;

- Collected
    - The source of the data, a form, an existing dataset etc
    - What data types are collected (name, address etc)
    - Who the data belongs to Student, Staff, School etc
    - Lawfulness of the processing (consent, contractual obligation see ICO guidance). Relying on consent may have additional requirements the compliance team will advise further on any PIA relying on consent
    - How Many people would be affected if there were to be a breach of GDPR due to this processing? (If this is variable provide an average of the number of people whose data is processed in a given academic year) This is required to define the severity/risk level of this processing.
- Stored
    - Data stored in the cloud (SaaS etc) Must be stored within the EEA
    - Ideally data should be stored within the UK
    - Data transferred/stored outside the EEA (and in some cases post Brexit, within the EEA) by the third party, must rely on "EU (unaltered) model GDPR contractual clauses", this must be specifically stated in any terms of service. Provide copies of such documentation with the PIA
- Used (processed)
    - How the data is used (decisions made based on data, outputs/results of the processing
    - Is the data shared with other third parties or subsidiaries of the university (requires sharing agreements or legal basis for sharing)

- Deleted (Retention)
    - Detail how long the data in whole or in part will be retained and the legal basis for both removing and retaining data. Refer to the university retention schedule where applicable as this will provide the classification of the data and in most cases the legal basis for the retention
    - Describe how the retention or deletion of data will be managed, this could be automatic or a manual process, describe the process, rules and staff training that will be used to enforce the correct retention of the data.
- Who has access to the data and how access is managed?
    - Access to personal data must be limited and proportionate, describe who will have access to the data
    - Describe how authorisation to change who has access will be managed (change control)

This step is a key part of any PIA process. A thorough assessment of privacy risks is only possible if an organisation fully understands how information is being used in a project. An incomplete understanding of how information is used can be a significant privacy risk – for example; data might be used for unfair purposes or disclosed inappropriately.

Where the processing involves third party software or services, ask the third party to assist as they will no doubt have a better understanding of their service and the technology that underpins it. Ensure any parties internal or external that are consulted are logged in the PIA under the consultation section below as good evidence of due diligence.

This part of the PIA process can be integrated with any similar exercises which would already be done, for example information project scopes, GDPR audits, student journeys or asset registers.

Step Two: Consultation

Key points:

- Consultation is an important part of the PIA and allows people to highlight privacy risks and solutions based on their own area of expertise
- It can take place at any point in the PIA process
- Internal consultation will usually be with a range of internal stakeholders to ensure that all relevant perspectives are considered
- External consultation provides the opportunity to get input from the people who will ultimately be affected by the project and to benefit from wider expertise

There is no set process for conducting consultation as it will depend on various factors, particularly the scale of the project, but PIAs can be integrated with other consultations or as discussion of the planning processes. This allows the University to consult the right people at the right time and avoid having to spend more time and resources on a separate exercise.

Internal consultation

Effective consultation with colleagues is an important part of any PIA. Data protection risks are more likely to remain unmitigated on projects which have not involved discussions with the people building a system or carrying out procedures.

Internal consultation can include informal discussions and emails, more formal project management meetings, and approval at board level. Most internal stakeholders will already have some level of involvement in the project – the aim of the PIA is to focus their attention on privacy issues.

Identifying internal stakeholders will be easier if the information flows have been described in detail, but some initial internal consultation may be needed to describe the information flow in the first place.

Examples of internal stakeholders to consider

- Students – It is important to maintain a transparent approach when dealing with student personal data, an appropriate communication plan and mechanism for feedback from students is clear evidence of transparency.
- Project management team - The team responsible for the overall implementation of a project will play a central role in the PIA process.
- Data protection officer - They are likely to have a close link to a PIA. Even if project managers are responsible for individual PIAs, the DPO will be able to provide specialist knowledge on privacy issues

- IT Engineers, developers and designers - The people who will be building a product need to have a clear understanding of how to approach privacy issues. They will also be able to suggest workable privacy solutions to the risks which have been identified
- Information technology (IT) - Will be able to advise on security risks and solutions. The role of IT is not limited to security, and might also include discussions on the usability of any software
- Procurement - If the project will require systems or services to be procured, the needs of the project need to be established before procurement takes place
- Potential suppliers and data processors - If some of the project will be outsourced to a third party, early engagement will help to understand which options are available
- Communications - A PIA can become a useful part of a project's communication strategy. For example, involving communications colleagues in the PIA can help to establish a clear message to the public about a project
- Student-facing/administrative roles - It is important to consult with the people who will have to use a new system or put a policy into practice. They will be able to advise on whether the system will work as intended.
- Corporate governance/compliance - Colleagues who work on risk management for an organisation should be able to integrate PIAs into their work. Other areas of compliance can be included in the PIA process.
- Researchers, analysts and statisticians - Information gathered by a new project may be used to analyse student behaviour or for other statistical purposes. Where relevant, consulting with researchers can lead to more effective safeguards such as anonymisation
- Senior management - It will be important to involve those with responsibility for signing off or approving a project.

External consultation

External consultation means seeking the views of the people who will be affected by the project. There are two main aims. Firstly, it enables the University to understand the concerns of those individuals. The consultation will also improve transparency by making people aware of how information about them is being used.

How extensive the consultation needs to be will be driven by the types of risk and the numbers of people affected. Existing consultation mechanisms such as focus groups, user groups, public meetings or student panels can, and should be used to gain a better understanding of privacy concerns and expectations.

External consultation also provides the opportunity for the University to benefit from wider views and from expertise that may not exist within the organisation itself.

Effective external consultations should follow these principles:

- Timely – at the right stage and allow enough time for responses.
- Clear and proportionate– in scope and focused.
- Reach and representative - ensure those likely to be affected have a voice
- Ask objective questions and present realistic options.
- Feedback – ensure that those participating get feedback at the end of the process

Step Three: Identifying privacy and related risks

A key principle of PIA is that the process is a form of risk management. When conducting a PIA an organisation is systematically considering how their project will affect individuals' privacy.

Privacy risks to individuals usually have associated compliance risks and risks to the University. For example, a project which is seen as intrusive or insecure by the public also increases the risk of fines, reputational damage, loss of business and failure of the project.

- Record the risks to individuals, including possible intrusions on privacy where appropriate
- Assess the corporate risks, including regulatory action, reputational damage, and loss of public trust
- Conduct a compliance check against the General Data Protection Regulation 2018, the Data Protection Act 2018 and other relevant legislation
- Maintain a record of the risks identified by way of the phase two form completion or link to a project risk register if applicable
- This demonstrates that the University is open about risks and aware of potential changes to projects
- Use the information flow from Step Two, collection, storage, Processing, Retention and access control, add a risk that could be associated with each of these as a starting point, imagine what happens if each stage went wrong what are the risks. retention schedule

Phase Two form Step Three;

- includes optional drop downs that include some of the more common Individual, Compliance and corporate risks. This list is not exhaustive enter any other risk identified as required. Further examples listed below
- Carries over risks logged in Step Three to Step 5 to remove the need to duplicate entries in the step 5 sign off section.

Examples of risks:

Risks to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary. retention schedule

Corporate risks

- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern if people are not engaged with the University from the outset and have not had the opportunity to be reassured of the protection of their data
- Public distrust about how information is stored can damage the reputation of the University and lead to loss of business.
- Non-compliance with GDPR or other legal obligation
- Biometric Information privacy

- Intrusive automated processing/decision making (AI)
- Insufficient Consent / Consent Management
- Data loss or theft
- Data storage outside the EEA
- Third party supplier compliance
- Third party sharing agreement

Compliance risks

- Non-compliance with the GDPR
- Non-compliance with the Privacy and Electronic Communications Regulation (PECR)
- Non-compliance with sector specific legislation or standards
- Non-compliance with human rights legislation

Step Four: identifying and evaluating privacy solutions

It is important to remember that the aim of a PIA is not to completely eliminate the impact on privacy. The purpose of the PIA is to reduce the impact to an acceptable level while still allowing a useful project to be implemented. The process of identifying and implementing changes should be integrated with the wider project development process. The aim of this stage of the process is to balance the project's outcomes with the impact on individuals.

- Devise ways to reduce or eliminate privacy risks
- Assess the costs and benefits of each proposed approach, looking at the impact on privacy and the effect on the project outcomes
- Refer back to the privacy risk register until satisfied with the overall privacy impact
- This stage records privacy risks which have been accepted as necessary for the project to continue

There are many different steps which organisations can take to reduce a privacy risk. Some of the more likely measures include:

- Deciding not to collect or store particular types of information.
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.

- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

The Phase two form can be used to record the implementation and subsequent changes to the level of risk. This stage should include the rationale for actions taken as the potential solution and the resultant effect on the risk level should be described in the evaluation field, describe why the solution is justified, compliant or proportionate

Step Five: Sign off and record the PIA Outcomes

Step 5 Risks are carried over from Step Three, the approved solution can be a reference from step 4 or an external supporting document if a more detailed description is required.

The 'Approved by' field must contain the name of the senior member of staff taking responsibility for the processing and will be the person contacted by the Data Protection Officer for any queries or issues related to the processing in the future. (Project Sponsor; Head of Team; member of the University Management Team)

Important note:
The Data Protection Officer and the compliance team will not formally sign off a PIA with a signature, however they will advise when PIA has been sufficiently completed. The PIA signoff is for the process owner to declare the processing is lawful by completing and signing the PIA.

The Data Protection Officer (DPO) has the right to object to processing commencing without a completed PIA and procurement may delay any purchase requests until a PIA is complete and confirmed completed by the DPO. It is recommended that PIAs are completed during the initial phase of new projects and as early as possible for processing that requires purchase requests to avoid any undue delays.

Step Six: Integrating the PIA outcomes back into a project plan

Although this section relates to a project, this is also applicable to informal projects, new suppliers and renewals etc as follow up tasks.

Formal Projects

- Ensure that all steps recommended by the PIA are implemented
- Continue to use the PIA throughout the lifecycle if the project when appropriate
- Ensure that all privacy solutions are carried out and documented
- Ensure that the PIA is referred to if the project is revised or expanded in the future

Most of the work required in a PIA will take place at the beginning and during the early stages of implementation of a project. However, care should be taken to ensure that the steps as a result of the PIA are properly implemented and are having the desired effect.

If the project aims develop or change during the project lifecycle, the screening questions may need to be revisited to ensure the PIA is still appropriate.

This can be done when other project reviews are taking place and where possible the PIA process should be developed to integrate with the University's other project management processes and methodologies.

Informal Projects, new suppliers, new services etc

List any follow up actions that may need to take place to ensure continued compliance.

For example, list tasks such as;

- Set reminders to review contracts and terms of service for third parties 1 month before the next renewal
- Review consent management yearly, quarterly as appropriate
- Ensure new staff and existing staff are trained on any processes
- Ensure documentation is up to date with process changes (Including the PIA)
- Ensure retention and deletions are processed as appropriate and lawful retention schedule

I have completed a PIA what happens now?

Conducting a PIA is primarily about the process of identifying and reducing risks. Those are the stages which will provide assurances that the University is using information in a way which is appropriate for their objectives and safer for individuals. However, it is also important to keep a record of the process. This will ensure that the necessary measures are implemented. It can also be used to assure the public, the ICO, and other stakeholders that the project has been thoroughly assessed.

Actions

- Email the completed form/s to recordsmanager@northampton.ac.uk for review
- The Compliance team will feedback on the submitted PIA and either;
    - Advise further changes
    - Approve the PIA as complete
- A copy of the PIA report or summary should be made available to the appropriate stakeholders for projects or management teams for non-project related activities
- The compliance team will store completed PIAs, these will be retained by the Data Protection Officer for auditing and GDPR compliance purposes
- Consider publishing the report or other relevant information about the process
- Ensure you set a reminder to review the PIA a minimum of yearly or prior to any renewal of service that will require a purchase request.