# Privacy Impact Assessment

## Introduction

A Privacy Impact Assessment (PIA) is a process which helps to identify and mitigate potential risks to privacy and compliance with data protection law when processing personal data.

Whilst there is currently no statutory requirement to undertake PIAs, they are regarded as good practice by the UK Information Commissioner's Office (ICO) and help to demonstrate compliance with existing data protection legislation. Under the new General Data Protection Regulation (GDPR), in force from 25 May 2018, PIAs are required for high risk processing activities.

## How does a PIA work?

A PIA enables organisations to identify and reduce the privacy risks of a project by analysing how the proposed uses of personal information and technology will work in practice.

## When is a PIA required?

Carrying out a PIA is mandatory where the processing of personal data is likely to result in a high risk to the rights and freedoms of individual data subjects.

You should consider conducting a PIA during the planning stage of new projects. A PIA may also be required if changes are made to an existing project.

Projects which might require a PIA include:

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.

- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding Automatic number plate recognition capabilities to existing CCTV).
- A new database which consolidates information held by separate parts of an organisation.
- A research project that involves the collection and analysis of personal data.
- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.

PIAs must be updated as the process develops, particularly if issues are identified which may affect the risk to the data protection rights of affected individuals.

**When is a PIA not required?**

It is not necessary to conduct a PIA in all circumstances. For example, a PIA would not be required where:

- The processing is not likely to result in a high risk to data subjects' rights;
- The nature, scope, context and purposes of the processing are very similar to the processing for which a PIA has already been carried out. Where a set of similar processing operations present similar high risks, a single PIA may be undertaken to address all of those processing operations; or
- Personal data is not being processed.

**How do I complete a PIA?**

The project initiator or project manager is responsible for completing the PIA. In the context of a research project, the Chief Investigator, Principal Investigator, or Supervisor is normally responsible for ensuring the completion of a PIA. You should use the template provided here [LINK].

## Who assesses the PIA?

You should submit your Privacy Impact Assessment form to the Data Protection Officer, who is the University Solicitor. Once you have submitted a PIA, the data protection team will assess the information that you have provided.

We will adopt a risk-based approach, considering what measures need to be put in place to protect the rights of data subjects and ensure UCA's compliance with data protection law in light of the risks involved.

As part of this assessment process, we may contact you and ask you to provide clarification on aspects of the PIA.

## Where can I find more information on PIAs?

You can find more information in the ICO' Code of Practice which can be found here.
https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf