Guide to completing a Privacy Impact Assessment

Under new Data Protection legislation GDPR - General Data Protection Regulation, it is necessary for all organisations to be more accountable and transparent with regard to the handling of personal data. Accountability is a new concept introduced by this legislation and will require DkIT as a data controller to be able to demonstrate how we comply with the data protection principles noted in DP legislation. This is highly significant as it shifts the burden of proof to the data controller in the event of a compliance investigation by the Data Protection Commissioner. As a result by May 2018 Institute personnel must carry out data protection Privacy Impact Assessments where the processing of personal data is likely to place individuals' rights at risk. This is a compulsory legislative requirement. GDPR contains a non-exhaustive list of instances which would require an assessment including when sensitive personal data is being processed. DkIT as well as being a data controller is also a data processor on a large scale so therefore need to comply with this element of the legislation.

It has always been good practice to adopt privacy by design as a default approach when handling personal information. Privacy by design and the minimisation of data have always been implicit requirements of the data protection principles. However the GDPR now enshrines both the principle of privacy by design and the principle of privacy by default in law. This in effect means that service settings must be automatically privacy friendly and requires that the development of services and products takes account of privacy considerations from the outset.

A PIA is essentially a risk assessment of proposed processing of personal data. It is the methodology to be used for assessing the impacts on privacy of a project, policy, programme, service, products or other initiative and in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or to minimise any negative impacts which might affect DkIT or individuals we engage with.

If you as a manager, staff member/researcher are processing personal data that might result in a high risk to the data subject's right, a PIA must be carried out prior to commencing that processing. If a data breach occurs, the Data Protection Commissioner, in conducting an

investigation, will request to view the Privacy Impact Assessment that was conducted for that particular process.

A PIA will need to be conducted where there might be high risks to an individual's rights and freedoms under Data Protection legislation. Most particularly it will be required where:

- New technologies are being introduced. Existing technologies should be reviewed to assess if a PIA is required.
- Any new kind of processing of data activities being undertaken
- There was no previous impact assessment in place
- A lapse of time has occurred a revised PIA may be required.

A PIA should not be undertaken in isolation, it is imperative that consultation with any stakeholders be undertaken and the Data Protection Officer should be involved in the process.

When to conduct a PIA?

A PIA is the process of systematically considering the potential impact that a project or initiative might have on the privacy of individuals. It will allow the Institute to identify potential privacy issues before they arise and come up with a way to mitigate them.

A PIA can involve discussion with relevant parties/stakeholders and can be as simple as noting in minutes that it was discussed during the course of a meeting and agreed upon. The level of discussion, deliberation and reporting will depend on the nature of the project or initiative. Discussion should involve the Institutes DP Officer. Ultimately whatever assessment is undertaken it may prove invaluable in determining the viability of future projects and initiatives. It also is mandatory in the following situations:

1. Where there is a systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.
2. Processing on a large scale of sensitive personal data. E.g. personal data that relates to students, and especially data pertaining to sensitive data which might relate to intellectual or disability needs pertaining to their studies or processing data from international students with regard to ethnicity.
3. Systematic monitoring of a publicly accessible area – e.g operation of CCTV in public areas.

Who has responsibility for conducting PIA?

The following are examples of Institute personnel who may have to conduct a PIA. (It is not an exhaustive list merely an indication)

- A project manager
- A research manager
- Senior academic managers' e.g. Heads of School, VP Academic Affairs/Registrar
- Senior non-academic managers including VPs Finance & Corporate Affairs, Strategy, Communication & Development
- Direct reports to the senior academic and non-academic managers such as Heads of Department and Heads of Function.
- Senior Administrative staff.
- External consultants

The Privacy Impact Assessment should include the following:

- Description of the operations undertaken
- Description of purposes for which the data will be collected and used
- Accountability and proportionality – accountability obligations may be greater where the organisation is responsible for processing personal data that pose a greater risk. More stringent measures will be required to be implemented by the organisation if this is the case.
- Risk assessment
- Measures to address any risks identified
- Measures to demonstrate compliance with GDPR such as ongoing reviews
- The Privacy Impact Assessment Template (attached) can be used to record the details of the risk assessment. As much information as possible should be recorded in this template and pertinent documentation appended as necessary.

Next step:

A findings report should be generated from the assessment which will identify the high risk areas and provide specific recommendations as to how to remediate each risk. Moreover, an overview of the risks against likelihood and severity should also be provided. This can be used going forward as a benchmark to demonstrate progress and data protection capability improvement.

Any risks noted should be fed into the Institutes Risk Register. This is a living document which should contain specific details on the risk, recommendations, next steps, actions-to-date, and the risk rating severity itself. This part of the output documentation becomes the 'active component' which should be systematically monitored, reviewed and updated.

If you are in any doubt if you should complete a PIA for any existing processes or initiatives or future ones, please contact Loretto Gaughran, FOI Officer on Loretto.gaughran@dkit.ie for further advice.