Parliamentary and Health Service Ombudsman

Data Protection Impact Assessment Procedure

Version 2 | November 2020

Purpose

Data protection impact assessments are a tool to constructively challenge whether we are making the best use of information, and if we do, are we doing so with considerately, lawfully and with appropriate safeguards in place.

This is good for the people whose information we manage as it reduces the risk of harm or distress through their privacy being invaded. This is also good for PHSO as it reduces the amount of information we need to store and safeguard and makes it more likely we can find what we are looking for.

Do I need to complete a DPIA?

If you are not planning on using personal information i.e. you are procuring ICT hardware like a monitor or furniture, you do not need to complete a DPIA. We have a screening tool that will help you determine this.

Personal information is information about or relating to people. Please find below some examples of when a DPIA will or will not be required.

Activity	DPIA?	comments
Upgrade corporate mobile phones	×	Low risk of harm to the rights and freedoms of individuals – changing the handset is about the device, not how its used
Monitor location of corporate mobiles	✓	High risk of harm to the rights and freedoms of individuals through location tracking of staff
Use biometrics e.g. fingerprints or face recognition to log into PHSO's network	✓	High risk of harm to the rights and freedoms of individuals as special category (very sensitive data like genetics, race, religion, or medical records) are being handled at scale
Ask successful applicants to provide their national insurance number	×	Low risk of harm to the rights and freedoms of individuals – this is necessary to pay them.
Asking all candidates to provide their National insurance number	✓	High risk of harm to the rights and freedoms of individuals as collecting this unnecessarily exposes those people to the risk of misuse.

Procedure overview

Data Protection laws (GDPR) require "privacy by design" to be at the heart of all activities which involve information about or that identifies people. We can demonstrate our compliance with this requirement by conducting Data Protection Impact Assessments (DPIA).

This is a formal approach to help us to properly identify and assess the risks to people from the way their personal data is collected, processed, shared, stored and disposed of. This is better for PHSO and the people whose information we handle as through reducing risk we make it easier to find the information we are looking for, reduce the cost of both paper and digital storage and protect ourselves against inadvertent mishandling.

Screening

PHSO has developed a screening tool which asks a series of questions that will inform whether you need to complete a DPIA.

If you can answer yes to any of these questions, you may need to complete a DPIA. If in doubt, please contact the DPO at dpo@ombudsman.org.uk

- Is the information about individuals likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?
- Will the initiative involve the collection of new information about individuals?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Will the initiative require you to contact individuals in ways which they may find intrusive or outside of activities documented in our privacy notice?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Does the initiative involve you using new technologies including those which might be perceived as being privacy intrusive e.g. genetic data, photographs or fingerprints?
- Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
- Will the change or proposal use systematic and extensive profiling or automated decision-making to make significant decisions about people?

- Do we intend to process special category data or criminal offence data on a large scale (big data)?
- Will we use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?
- Will we combine, compare or match data from multiple sources?
- Will we process personal data in a way which involves tracking individuals' online or offline location or behaviour?
- Do we intend to process personal data which could result in a risk of physical harm in the event of a security breach?
- Systematic processing of sensitive data or data of a highly personal nature.
- Are we intending to handle data concerning vulnerable data subjects?
- Are we putting in place innovative technological or organisational solutions?
- Could what we are doing prevent people from exercising a right or using a service or contract?

If in doubt, ask… **++DPO@ombudsman.org.uk**

3 DPIA procedure

The Information Commissioner's Office (ICO) identifies the following steps.

- We describe the nature, scope, context and purposes of the processing.
- We ask our data processors to help us understand and document their processing activities and identify any associated risks.
- We consider how best to consult individuals (or their representatives) and other relevant stakeholders.
- We ask for the advice of our data protection officer.
- We check that the processing is necessary for and proportionate to our purposes and describe how we will ensure data protection compliance.
- We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.

- We identify measures we can put in place to eliminate or reduce high risks.
- We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.
- You should start the process early as possible within design and implementation phases, to provide PHSO with visibility about risks to personal data that may exist within the activity. It will be easier and more cost effective to make privacy-related changes prior to the activity being launched, and before any personal data is processed by the activity.
- Any PHSO activity that changes from its original purposes needs to have an updated DPIA performed. The standard management report template now includes a data protection impact assessment section so that proposals and changes substantial enough to require formal approval or reports will include DPIA as standard. In addition, the PMO handbook has also been updated to describe both DPIAs and the responsibilities of project boards.
- Once the DPIA has been completed and finalised, the DPIA should be reviewed by both the DPO and DPIA owner to understand any observations or issues that have been identified. With the DPO having visibility of all DPIAs they will quickly identify any common shortcomings or issues that can be remediated centrally, for example by establishing a common policy, or improvements to training or technical controls.

4Step by step guide

4.1 STEP 1 | SCREENING

- When the data protection (also known as privacy') impact assessment screening tool is completed, send to the DPO at ++DPO@ombudsman.org.uk

4.2 STEP 2 |IMPACT ASSESSMENT

- If the DPO decides a privacy impact assessment is needed, you must complete one. The DPO will review the completed DPIA, record their advice (6) and inform the SIRO. The SIRO is the officer accountable for information risk within PHSO who makes the decision on how to manage or accept risks to people's information rights.
- This decision which will be either stop, proceed with caution/amendments or proceed will need to be followed. If the decision is either 'do not proceed' or 'proceed with amendments', any future proposal which is a revision of the proposal that has been rejected needs to go through the full privacy impact assessment process again.

- If the DPO does not think you need to complete a full privacy impact assessment, they will advise you accordingly and inform the SIRO.

4.3 STEP 3 | APPEAL

- The DPO will or reject completed DPIAs or screening tools. If the latter, they will communicate to the DPIA owner the reasons for their rejection, and require that an updated or amended assessment is completed without delay. As the DPO provides advice to PHSO on data protection, if you disagree with the advice given, you can make a representation to the Senior Information Risk Owner (SIRO). This will be via a formal agenda item at the Senior Information Risk Group.

4.4 STEP 4 | IMPLEMENT

- Measures identified during the DPIA process must be integrated them into the project plan or work stream. Project SROs are accountable within the project for ensuring that this is completed effectively.

4.5 STEP 5 | COMMUNICATE

- All DPIAs will be accessible to the Senior Information Risk Group and summaries published on www.ombudsman.org.uk as part of our publication scheme unless in exceptional circumstances. Person identifiable data except for senior managers at grade 2 and above (Assistant Directors) should be removed as standard.

- The ICO may ask to see DPIAs at any time and we are also obliged to consult with them before processing if we cannot mitigate high risks. Realistically, it is very unlikely that this will be the case.

4.6 STEP 6 | REVIEW

- Information Asset Owners (IAOs) and DPIA owners should review when appropriate, using the previous response as a basis for reviewing or making minor amendments to the PIA, although if major changes have taken place, it may prove more productive to prepare the new assessment from a blank template.

5 RESPONSIBILITIES

Everyone who works with or for PHSO should:

- Understand the important of treating people's information with respect and the role of data protection impact assessments in enabling that considerate handling.

- Only undertake their data processing activities strictly in accordance with the most recently published DPIA
- If they identify an issue or error within a DPIA report, are to notify this immediately to the PHSO DPO so that the PIA can be re-assessed

Senior Information Risk Owner

The SIRO is responsible for:

- Ensuring that PHSO remains fully compliant with GDPR
- Providing appropriate resources for the conducting of data protection impact assessments
- Providing guidance to the DPO on escalated issues arising from DPIA reports

Information Asset Owners

PHSO information asset owners must:

- Become proficient in conducting DPIAs of the activities, assets and projects for which they are responsible
- Ensure that their activities are properly and accurately assessed within the timeframe required by the PHSO
- Cooperate with the DPO and other activity owners in designing and implementing remedial actions
- Project Senior Responsible Owners or Sponsors SROs and Sponsors must:
- Ensure that DPIA screening and any necessary DPIAs are carried out at appropriate stages of their projects.
- Ensure that their activities are properly and accurately assessed within the timeframe required by the PHSO and the ICO.
- Cooperate with the DPO and other activity owners in designing and integrating agreed remedial measures into project plans.

Data Protection Officer

The DPO is responsible for:

- ensuring the PHSO implements and maintains an active programme of privacy impact assessments which meet the standard required by GDPR

- provide a programme of training, education and support, such that assigned activity owners can complete PIAs promptly and to an acceptable standard.
- provide advice and guidance to external organisations, for example third party data processors, who are required to contribute to the PHSO's PIAs
- evaluate the results of completed PIA reports, to identify and implement any remedial actions deemed necessary, and to escalate to the Board where appropriate
- co-ordinate the issue of the latest PIA reports within the PHSO, to stakeholders, relevant third parties and to data subjects upon request
- The PHSO Data Protection Officer (DPO) maintains a list of PHSO activities, and the assigned individuals who are responsible for conducting the PIA. Once assigned, they should work through the various sections to compile the PIA report as soon as possible.

Procedure information

Author: Angharad Jackson, Data Protection Officer

Version control

Date	Version	Content/changes made	Owner of changes
03/12/2020	2	Clarified when a DPIA is not necessary	Angharad Jackson

Parliamentary and Health Service Ombudsman

Citygate
Mosley Street
Manchester
M2 3HQ
United Kingdom

Telephone: 0345 015 4033

Textphone: 0300 061 4298

Fax: 0300 061 4000

Email: phso.enquiries@ombudsman.org.uk

www.ombudsman.org.uk

Follow us on:

If you would like this document in a different format, such as Daisy or large print, please contact us.