FERRYHILL
SCHOOL

Data Protection Impact Assessment Policy and Procedure

Policy Responsibility: Mrs L Edgar

Introduction

Data Protection Impact Assessments (also known as Privacy Impact Assessments or DPIAs) are an integral part of taking a 'privacy by design' approach. A DPIA is a process which minimises the privacy risks of new projects or work activities by considering the impact that the proposed project or activities will have on the individuals involved to ensure that potential problems are identified at the outset and addressed.

This guidance is based on comprehensive guidance produced by the Information Commissioner's Office which can be accessed at:

Click to view ICO information

When is a PIA required?

You must carry out a DPIA whenever you are implementing or making a change to a process or system, project or work activity that could have an impact on the privacy of individuals.

Stages of a PIA

Stage 1 - The initial screening questions

The purpose of the screening questions is to assess whether a further DPIA assessment is required**.**

- If the answers to the questions are no **-** the screening process has not identified any DPIA concerns and the process is complete
- If response to any of the questions is "yes" then a DPIA must be undertaken

It is important to get this stage right; if we are challenged by the Information Commissioner we have to be able to defend the decision about why we did or did not undertake a DPIA.

Stage 2 – Privacy Impact Assessment

The responses to the screening questions will give an indication as to the appropriate scale of the DPIA. In some cases, the answers to the screening questions may not be known and the process will need to be re-visited when more information comes to light.

The DPIA (Appendix B) must be completed by the person responsible for delivering the proposed change or new project. A copy of the completed form must be sent to the Data Protection Officer (info@mobile-sbm.com) to provide further guidance if necessary. There are three possible outcomes to the initial DPIA:

- The initial DPIA is incomplete and will have to be repeated, or further information obtained.
- The initial DPIA is complete and no privacy risks have been identified.

- The initial DPIA has identified privacy risk(s).

If the DPIA had identified a Privacy Risk, an action plan must be developed on how the risks will be mitigated. This will include identified issues, associated actions, related roles and responsibilities and timescales.

Measures to reduce the risk

It is important to remember that the aim of a DPIA is not to eliminate the impact on privacy. The purpose of the DPIA is to reduce the impact to an acceptable level while still allowing a useful project to be implemented.

Examples of measures:

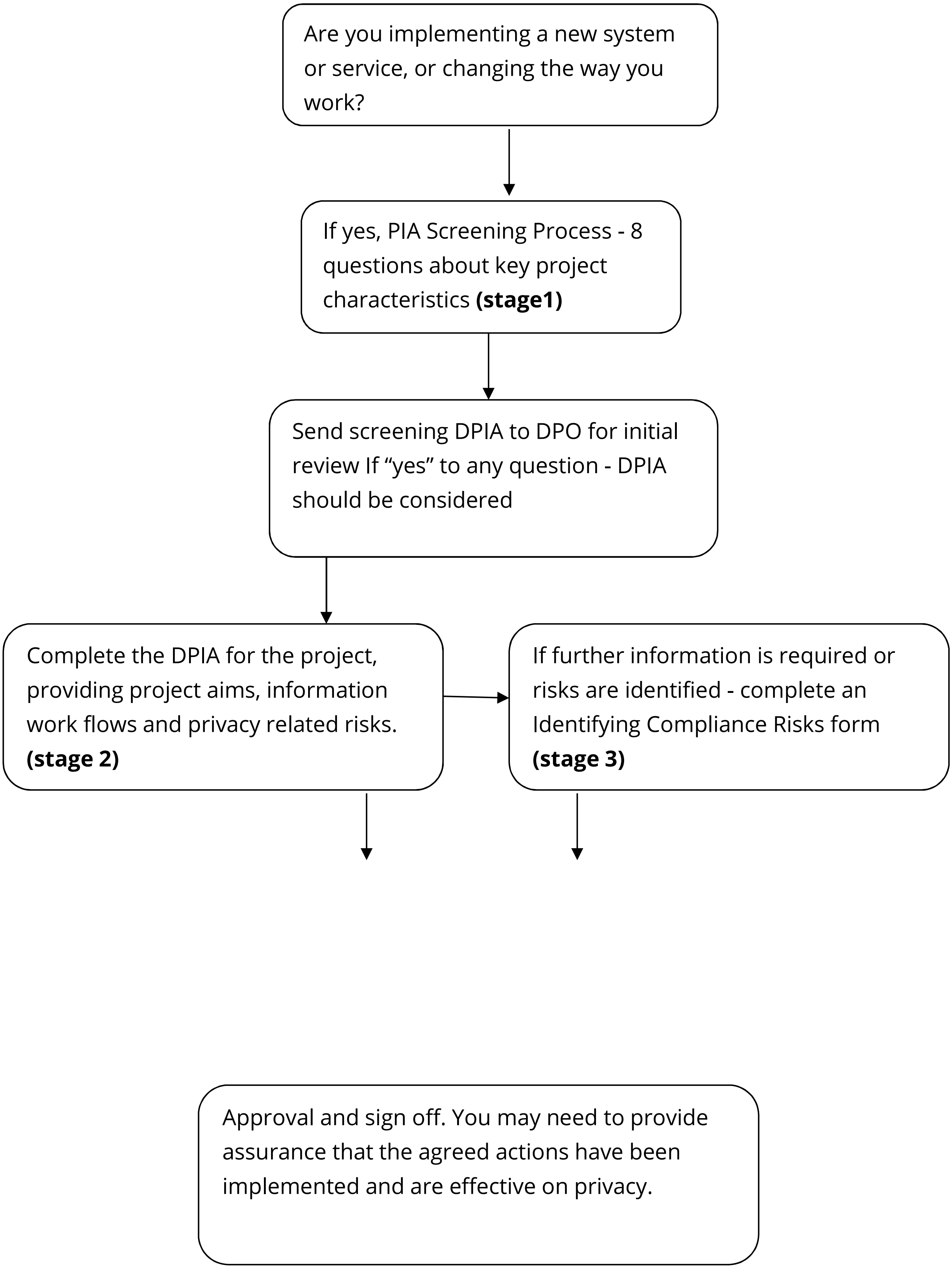
- Obtaining the data subject's consent;
- Deciding not to collect or store particular types of information;
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information;
- Implementing appropriate technological and organisational security measures;
- Ensuring that staff are properly trained and are aware of potential privacy risks;
- Developing ways to safely anonymise the information
- 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 how to contact the DPO 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 the Academy'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.

Integrating the DPIA outcomes back into the project plan

The DPIA findings and actions should be integrated with the project plan. The person responsible for the DPIA and the overall project should ensure that the steps recommended are implemented and return to the DPIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.

If the DPIA generates actions which will continue after the assessment has finished, the person responsible should ensure that these are monitored and that all lessons learnt from the DPIA are recorded for future projects.

Flowchart



Are you implementing a new system or service, or changing the way you work?

If yes, PIA Screening Process - 8 questions about key project characteristics **(stage1)**

Send screening DPIA to DPO for initial review If “yes” to any question - DPIA should be considered

Complete the DPIA for the project, providing project aims, information work flows and privacy related risks. **(stage 2)**

If further information is required or risks are identified - complete an Identifying Compliance Risks form **(stage 3)**

Approval and sign off. You may need to provide assurance that the agreed actions have been implemented and are effective on privacy.

Appendix A

DPIA Initial Screening Form

Project name:		Date:
Brief project outline:		
Project Lead Officer:		

DPIA Screening Questions

These questions are intended to help decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise.

Once completed please return to the DPO for review:

Question	Yes/No (√)		Notes
Will the project involve the collection of new information about individuals?	**Y**	**N**	
Will the project compel individuals to provide information about themselves?	**Y**	**N**	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	**Y**	**N**	
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	**Y**	**N**	
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	**Y**	**N**	
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	**Y**	**N**	

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	**Y**	**N**	
Will the project require you to contact individuals in ways which they may find intrusive?	**Y**	**N**	

DPO FEEDBACK/DECISION:

IGT USE ONLY:

DATE:

OFFICER:

Policy Responsibility: Mrs L Edgar

Appendix B

This Appendix is a template DPIA Form to be used to record DPIA process and outcome. It follows the process set out in the ICO's DPIA guidance.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, DPO may consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		

Policy Responsibility: Mrs L Edgar