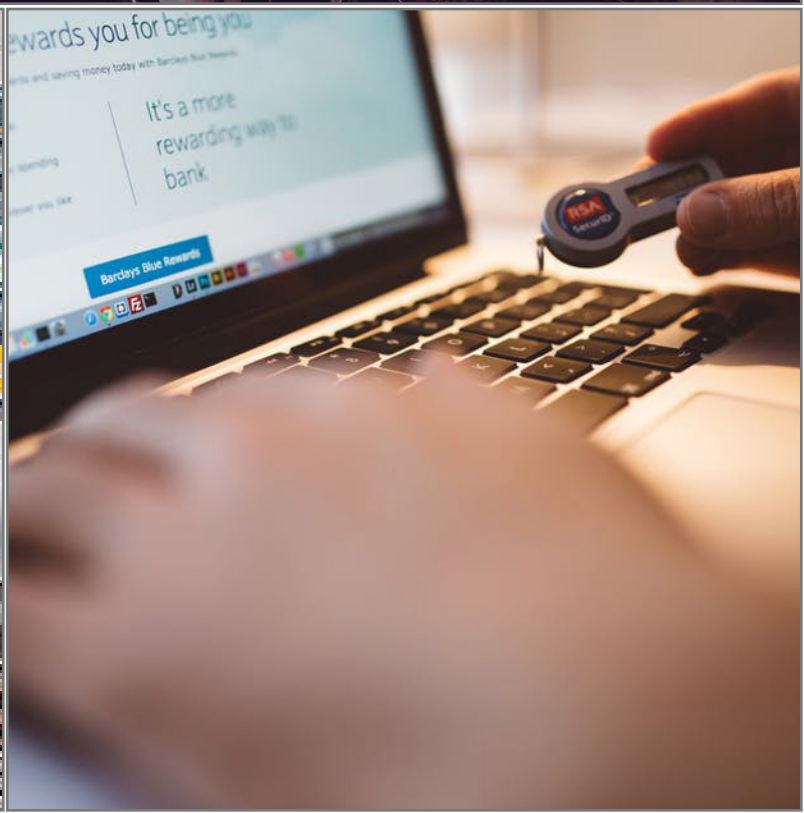
DPIA POLICY



Contents

1. PIA Policy

1.1 What are Privacy Impact Assessments?

1.1.1 The Information Commissioner defines a privacy impact assessment as a process which helps an organisation to identify and reduce the privacy risks of a project We call them PIAs for short.

1.1.2 Personal information may sometimes be required to be collected or processed as part of a new business process, or a change to an existing business process (a "**change**").

1.1.3 Our policy is that a PIA should be carried out for all new projects involving personal data. This includes the use of new suppliers (or contract renewal), new databases and computer systems, using personal data in new ways and using data in a potentially privacy intrusive or risky way. It is a fundamental part of our requirements to ensure privacy by design and default.

1.1.4 The first step is to complete and return the PIA screening questions (appendix 1). The PIA screening questions should be returned to the DPO, who will work with the Data Protection Manager in assessing whether a full PIA is required

.
Appendix 2 contains the template for a full data protection impact assessment ("DPIA"). Where a full DPIA is required, it will form an integral part of the early stages of any project and will continue to be used throughout the development and implementation of the project. The full DPIA will be completed by the project lead in conjunction with the DPO. It is recommended that you engage directly with the DPO at the earliest stage of any project or change so that the DPO can assist you with the completion of the PIA

1.2 When must I carry out a Privacy impact assessment?

1.2.1 You must complete the PIA screening questionnaire at the start of any new project, retendering process, if you are thinking about collecting or using personal data for new reasons or are considering any kind of systems update (such as a new email provider, data base or new CCTV installation)

1.2.2 Completion of the PIA screening questionnaire will indicate whether the full DPIA is required. The DPO will provide advice about any privacy measures which are required.

1.3 Who is responsible for Privacy impact assessments?

1.3.1 The person responsible (the project lead) for the project must submit the PIA screening questionnaire to the DPO preliminary who will then assess whether a full PIA is required or whether they are content with the proposal or whether they can recommend privacy controls without the needs of a full PIA.

1.3.2 If required, the person responsible for delivering such change shall complete the Privacy Impact Assessment ("**PIA**") The PIA should be completed and given to the DPO in sufficient time for the DPO to provide comments on the compatibility of the change with the requirements of the Law.

1.3.3 If any proposed change is found not to be compatible with the DPL, the business and the DPO shall collaborate to amend the proposed change so it does not breach the DPL.

1.3.4 The DPO must be allowed to lodge a dissenting opinion with the Board. The Project Board and Change Management Board are responsible to ensure no
project or change is put into operation unless the steps required as part of the PIA are carried out.

1.3.5 The Project's Executive Sponsor is accountable to the Board of Directors for ensuring that each new Project complies with Data Protection Law.

1.3.6 The Project Change Board will not approve projects unless the PIAs are been carried out in accordance with the policy and procedure.

1.3.7 Procurement will not approve new contracts or purchase orders unless the requirements for PIAs are being followed.

1.3.8 The Data Protection Manager must be consulted in relation to all PIAS in their organisation and can refer queries and decision to the DPO.

1.3.9 The DPO must be consulted in relation to all PIAs

2. PIA Procedure

2.1 How to complete the PIA

The templates for the PIA Screening Questionnaire and PIA are attached in Appendix A and Appendix B. All PIAs need to be sent to the DPO in a timely manner to allow review and consultation. A separate PIA is established for CCTV in line with guidance from the Surveillance Camera Commissioner.

2.2. How to keep a copy of the PIAs

2.2.1 The DPO will keep a record. The project should retain copies with the other documentation relating to the project. Where a PIA is carried out in relation to a supplier, then a copy should be retained on the procurement database along with a copy of the contract.

2.2.2 The project and director in charge of the directorate is responsible for ensuring the DPM/DPO has the information required to provide advice about data protection compliance.

2.3 Considerations for assessing risk

2.3.1 The PIA will assess the risks associated with any project or change which will include carrying out a Security Risk Assessment (CIA). This may involve consultation with the IT Team and Information Security Team about systems capabilities and security controls. Risks will be assessed against likelihood and impact and appropriate controls put in place to manage these risks.

Appendix 1

PIA Screening Questions

Will the project involve the collection of new information about individuals?

Will the project compel individuals to provide information about themselves?

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

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.

Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

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.

Will the project require you to contact individuals in ways which they may find intrusive?

Appendix 2

Full Privacy Impact Assessment

To be completed by Project Lead and sent to the DPO for review

Project Name	
Project Description	
Date PIA undertaken	
Review Date(s) (if any)	
Date PIA concluded	

Step 1: Project or change overview

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.

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 s? 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/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, 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:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA