

Sample DPIA template



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.

Independent custody visitors – a scheme administrated by the OPCC whereby volunteers attend at police custody suites to check on the welfare of detainees. Personal data will be involved in the administration of these scheme, with the general management of volunteers being managed in-line with the organisation's recruitment policies and procedures.

The project will involve the collection of data for recruitment purposes in order to fulfil the OPCC's public task of holding the police to account, namely with regard to the fair treatment of detainees in their custody suites.

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?

Data will be collected direct from individuals. It will be processed for the purposes of administrating their application, and not shared with anyone else. There is no high risk processing.

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?

The data will be collected from the individual – there is a monitoring questionnaire as part of the application, but this will be anonymous and kept separate from the main form. We will retain the data of successful applicants until six years after they leave. Unsuccessful applications will be retained for six months then permanently disposed of. Applicants will be from the Humberside Police force area and generally there are approximately 5 new applications per year (if there is not a targeted recruitment event) and there are approximately 25 active ICVs at any given time.

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)?

Individuals will be volunteers for the OPCC. They don't have a contract of employment but do sign a memorandum of understanding of what each party can expect from one another. Although this is not a formal contract, there is an imbalance of power in that the OPCC is a public authority. Essentially, the processing is the same as an application for a job which is not unusual for applicants to go through.

There is some collection of third-party details, namely next of kin in case of emergency. There is a note on the application form to ensure that the data subjects have agreed for their details to be used only for this purpose.

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?

The overall purpose is to administrate the ICVs, ensuring that we have up-to-date contact details and that the scheme operates smoothly.

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?

No consultation is required.

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?

Lawful basis is public task – in the PCC code of practice under the Police Reform Act 2002. The processing is of only enough data to manage the ICVs.

Data quality will be maintained by way of the data coming from the data subject direct, and they are asked to notify us of any changes.

Individuals will be given a privacy notice at the point of data collection, on the form on which they provide their details.

There are no processors nor 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
<p>Personal data is compromised by way of an intentional or inadvertent disclosure by OPCC staff.</p> <p>Next of kin data is compromised or disclosed for a purpose other than which it was collected.</p>	<p>Remote, possible or probable</p> <p>Remote</p> <p>Remote</p>	<p>Minimal, significant or severe</p> <p>Significant</p> <p>Significant</p>	<p>Low, medium or high</p> <p>Low</p> <p>Low</p>

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
Data Breach	Fully vetted staff	Eliminated reduced accepted	Low medium high	Yes/no
		Accepted	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Mia Jones	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Rachel Cook	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Mike Richmond	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Check privacy notice is adequate and that any monitoring data is kept separate from personal data in the application process.		
DPO advice accepted or overruled by:	Accepted by Rachel Cook	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
--------------------------------------	--	---