

DPIA: Police Complaints Appeals



Step 1: Identify the need for a DPIA

<p>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.</p>
<p>The OPCC wishes to engage an external contractor as a Data Processor to assist with handling reviews of the outcomes of Police Complaints. This will involve the transfer of Personal Data and potentially Law Enforcement Data obtained from Humberside Police to a third party, in order for them to review how the complaint was handled and make a recommendation for a relevant officer in the OPCC to respond to the review.</p>

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?

The data will be provided by Humberside Police over secure email, and when the services of a contractor are engaged, shared with them via secure email. This involves the handling of personal data about the member of the public who made the complaint, the officer(s) involved in the incident, members of staff in the Professional Standards Department (PSD) who handled the initial complaint and any witnesses to the events subject to the complaint. Data will be retained by the processor for the purposes of dealing with the review, and deleted no longer than six months after the review has been completed and the complainant informed of the outcome.

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 could potentially include criminal offence data, insofar as it is directly relevant to the complaint. The data will include some or all of the following:

- Original complaint submission (could be a log, online document or in writing)
- Assessment and Recording Form completed by PSD
- All correspondence to and from the complainant in relation to the handling of their complaint
- All correspondence to and from PSD in relation to the handling of the complaint
- Final outcome letter from PSD to the complainant
- Evidence or information which has been considered/weighed/reviewed/assessed during complaint handling – this could include for example a policy, investigation report, incident log, audio file, information relating to the investigation or outcome of a previous complaint, BWV – it's dependent on the nature and context of the original complaint.

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 contacted by the OPCC at the point of the complaint review being received, and periodically contacted throughout the processing of their review until such a time as a final outcome decision is made and communicated to them. Several other OPCCs and other agencies engage a third-party contractor in this way.

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 purpose of the processing is to comply with the OPCC's legal obligation to review the outcomes of police complaints where there is an appeal. The reason for engaging a third-party processor is to ensure that the complaints appeals are reviewed fairly by an independent, trained member of staff, in a cost-effective way and to ensure that members of the public receive a prompt service.

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?

The police will be made aware that the data they provide will be used in this way. The public would reasonably expect that the OPCC – as the body to which they appeal against an outcome – to process their personal data. The OPCC will make clear that Personal Data may be processed by a subcontractor in its privacy notice.

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?

The lawful basis for processing this information is a legal obligation of the OPCC under Section 29 Police Complaints and Misconduct Regulations 2020 and Paragraph 25 schedule 3 Police Reform Act 2002. OPCC staff are not able to manage the volume of complaints without additional support. A Data Processing Contract will be put into place to ensure that the requirements of GDPR Article 28(3) are met.




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>Data breach exposes personal data of data subjects</p> <p>Breach of confidentiality</p> <p>Breach during data transfer</p>	<p>Remote, possible or probable</p> <p>Possible</p>	<p>Minimal, significant or severe</p> <p>Significant</p>	<p>Low, medium or high</p> <p>Medium</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		Eliminated reduced accepted	Low medium high	
	Ensure all contractor staff are vetted	Reduced	Low	Yes
	Contractor to assure OPCC of information governance policies and disciplinary policies	Reduced	Low	Yes
	Ensure appropriate technical measures are in place for information transfer	Reduced	Low	Yes
	Retain all work in-house	Reduced	Low	No

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	 Rachel Cook 23/9/2020	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	 Rachel Cook 23/9/2020	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Michael Richmond 16/9/2020	DPO should advise on compliance, step 6 measures and whether processing can proceed
<p>Summary of DPO advice:</p> <p>The following safeguards must be put into place:</p> <ol style="list-style-type: none"> 1. The OPCC must provide complainants with a Privacy Notice that makes clear that their personal data will be transferred to a third-party for processing. 2. A Data Processing Contract is required under the GDPR Article 28(3), and must meet the requirements therein. 3. The OPCC must ensure that the contracted organisation has appropriate policies and training in place regarding data protection, that its staff are vetted to the standards required and must maintain the right to audit compliance. 		
DPO advice accepted or overruled by:	 Rachel Cook 23/9/2020	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