Police Complaint Reviews DPIA

This DPIA follows the process set out in ICO DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

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.
Phase 3 of the Police Complaints Reforms gives Local Policing Bodies responsibility for undertaking reviews (formerly complaints appeals) where they are the Relevant Review Body. Legislative changes give complainants a single right to apply for a review of the outcome of their complaint. In order that Home Office and IOPC data collection requirements can be met and to ensure a streamlined administrative process with effective 'data flow' it will be necessary for the OPCC to access complaints records (and to record review outcomes) via Centurion, the case management system currently used by PSD to record and progress police complaints. In order that the OPCC can provide a transparent and impartial service to the public and effectively manage demand in a way that offers value for money, we will use an external contractor who will provide the services of an Independent Review Officer (IRO). Thie will involve the transfer of Personal Data and Law Enforcement Data obtained from Humberside Police to a third party. This is required in order for the IRO to review how the complaint was handled and make a recommendation to the OPCC regarding the review outcome. The OPCC will use the contracted services of Sancus Solutions for the provision of an Independent Review service. A Decision Record is in place for this contractual arrangement.

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 can be viewed within Centurion by named officers within the Statutory/Assurance function at the OPCC, with access granted and managed by PSD. For the undertaking of Reviews, relevant case data will be made accessible by Humberside Police PSD using the secure data platform Egress. PSD will create a folder in Egress and provide a link to that folder, by email, to the relevant officer at the OPCC. The link will be shared by email with the IRO when the services of a contractor are engaged, for the purposes of undertaking an independent review. Permissions for access to the Egress case is controlled and locked down by PSD. Accessing police data using this secure method negates the need to save or retain by the OPCC or Independent Review Officer. Data will be used to communicate with the complainant and to assess the handling and outcome of the complaint, with a view to upholding/not upholding the review. Data comes from either the complainant (upon receipt of a review) or from records made or collated by the initial PSD complaint handler. Data which can be accessed includes 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. Should it be determined that the LPB is not the Relevant Review Body (RRB), the matter is referred to the RRB as directed by IOPC Statutory Guidance. This does not require consent though complainants will be informed where such cases arise. Data comes from either the complainant (upon receipt of a review) or from records made or collated by the initial PSD complaint handler.

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?
Data will include complainant details (name, address, email address, telephone number, DOB) Data may include identifying details of police officers or police staff against whom a complaint has been made. Data may include incident details (log entries) Data may include statements (complainant, witness, police officer, staff) and may include criminal offence data, should it form part of the circumstances surrounding an initial complaint. Date will include some or all of the following: • Original complaint submission (log/online document/transcript/written) • Assessment and Recording Form completed by PSD • All correspondence between the complainant and PSD complaint handler • All correspondence between the complaint handler and other Force members • Final outcome letter with explanation, considerations and outcome • Evidence which has been weighed/considered/reviewed/assessed during complaint handling – this could include for example a policy, investigation report, incident log, audio file, information relating to an investigation or outcome of a previous complaint, Body Worn Video Data will be made available via link to Egress upon notification of a valid Review application, which the OPCC provides to PSD following an initial validity check. Because complainants have the right to Review upon conclusion of any complaint allegation, it is challenging to estimate anticipated case demand. There are no geographical limitations.

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)?
A named individual at Sancus Solutions will undertake the independent review function, the primary role of which is to ensure that the outcome of a complaint is both reasonable and proportionate. It is possible that Data Subjects may include children or vulnerable groups. Administration of the review process will be undertaken by suitably trained staff within the OPCC Statutory Operations/Assurance team. This will include all contact and correspondence with the complainant; before, during and after the review. The outcome of the review will be shared with the complainant and with the Appropriate Authority via PSD. PSD take responsibility for providing updates to officers and staff who may be the subject of complaint allegations. 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. Information pertaining to complaint handling is accessed only for the purpose of the review, which is undertaken only following formal request by the complainant.

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 a valid application for review. The reason for engaging a third-party processor is to ensure reviews are undertaken fairly and impartially, in a cost effective way which delivers value for money, supports demand management, and provides a high level of public service. The intended impact on individuals is that they will have confidence that their concerns are being reviewed independently of the Force, with a fair and transparent outcome. More broadly, benefits to the public include increased confidence in the Police Complaints system and for the Force, development as a learning organisation.

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?
A significant amount of consultation has been undertaken by the Home Office, FIS (Centurion) and the IOPC in developing upgrades to Centurion which have been created to reflect the new Regulations – including the Review process. Humberside Police are aware that the access to data they provide will be used to support the Reveiw function. The public would reasonably expect that the OPCC – as the relevant review body – must process their personal data. The OPCC will make clear that Personal Data may be processed by a third party in its privacy notice and FAQs.

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 data processing is that of Public Task. Parameters for undertaking police complaint reviews are clearly defined within Home Office Regulations and IOPC Statutory Guidance and subsequently 'function creep' is unlikely to occur. Reference is given to section 29 Police Complaints and Misconduct Regulations 2020 and Paragraph 25 schedule 3 Police Reform Act 2002. Responsibility for data accessed for the purposes of Reviews remains the responsibility of the Force and issues or concerns regarding data quality will be referred appropriately.

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**
Loss, theft or disclosure of personal data	Possible	Significant	Medium

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:	Rachel COOK	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	N/A	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: •		
DPO advice accepted or overruled by:	Rachel COOK	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	N/A	If your decision departs from individuals' views, you must explain your reasons
Comments:		

This DPIA will kept under review by:	Clare Rex	The DPO should also review ongoing compliance with DPIA

Reviewed Jan 21 (CR) – changes recorded within document
Reviewed Jan 22 (CR) – no change
Reviewed Jan 23 (MR) – no change
Reviewed Jan 24 (MR) – no change
Reviewed Jan 25 (MR) – no change
Reviewed Jan 26 (CR)