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.

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 viewed, retrieved and recorded within Centurion by the Statutory Operations Manager. Data will be used to communicate with the complainant and to assess the review with a view to upholding/not upholding it Data would not routinely be shared with third parties. However, should it be determined that the LPB is not the relevant review body, the matter must be referred to the relevant review body as directed by IPOC Statutory Guidance. This does not require consent though complainants will be informed where such cases arise. Data would be deleted as part of PSD's weeding policy (a review would not be deleted until such a time as the initial complaint is deleted in line with Force Data Retention Policy. Guidance on weeding rules are provided to the Force by the IOPC) Data comes from either the complainant (upon receipt of a review) or from records made 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 who 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. Data will remain within Centurion and will not be stored separately on OPCC systems. Centurion workflow will be 'locked down' to enable access only to those cases for which the LPB (OPCC) is the Relevant Review Body. Data will be accessed upon receipt of a valid Review application – complainants have the right to Review upon conclusion of any complaint allegation. It is difficult to estimate the anticipated number of Reviews to be undertaken under the newly defined Regulations. 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)?
The Statutory Operations Manager will undertake the independent reviews function, the primary role of which is to ensure that the outcome of a complaint is both reasonable and proportionate. Data Subjects would expect their data to be accessed in this way during the course of the review of their complaint outcome. It is possible that Data Subjects may include children or vulnerable groups. The Statutory Operations Manager is not aware of any prior concerns over this type of processing or security flaws. The role has previously been undertaken within former Regulations (in place until 31 Jan 2019) by the Force solicitor, who has been able to access the same data. Centurion is a secure, licensed complaints and case management system which is used by the majority of Forces nationally and will be accessed by the majority of OPCCs when the Regulations change on 01.02.20.

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 aim is to achieve a fair and transparent review of a complaint outcome at the request of a complainant, to ensure that the Force has dealt with their complaint reasonably and proportionately. 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. The benefits of processing for the OPCC are that we are able to comply with our statutory obligations to undertake this role under the new Regulations – and also to increase our scrutiny in terms of complaint handling, with an additional role of making recommendations to the Force. More broadly, benefits to the public are increased confidence in the Police Complaints system and for the Force, development as a learning organization.

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. Awareness days are taking place to train relevant OPCC staff to use Centurion v7.0 and ongoing training will be rolled out by the PSD Centurion Administrator. Further consultation is not necessary and would be of no benefit.

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. 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	Remote	Significant	Low

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: • No data protection concerns with proposed course of action		
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:		The DPO should also review ongoing compliance with DPIA