Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

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.
The project will involve contracting an external agency to: • review current HR policies and procedures (including systems) • review current terms and conditions of employment and employee personal files for 16 staff currently working in the OPCC for Humberside • deliver refreshed/ modernised HR policies and procedures • review options appraisal of wider opportunities – including enabling workforce tools such as agile working, performance related pay. As part of the project, data will be transferred from Humberside Police systems to the OPCC systems. A regional DPIA screening has been completed which recommended the need for a DPIA under the following criteria: • Some personal information will be transferred between two secure systems • Some contractual information will be accessed as part of the work

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?
Existing data about OPCC personnel will be used. The data will potentially include of: • Names • Dates of Birth • Addresses • Employment details e.g payroll number, post and pay scale • Contracts of employment • Details of absences from work It will be transferred from the Humberside Police HR System into the OPCC system via secure email, and accessed via vetted contractors working for CPD Consultancy Group Limited. Personal data will only be accessed and viewed within OPCC premises, using OPCC machines and will not be transferred out, printed, saved to removable media or otherwise transferred onward to any other party. The consultancy work will be looking at opportunities to change terms and conditions, which will involve viewing and aggregating information from records containing personal data

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 may include sensitive personal information such as gender, marital status, salary details and reasons for absence from work. It will only be viewed in order to understand the range of terms and conditions of employment in-place for the OPCC staff in order to understand similarities and differences and identify opportunities for improvement or efficiency. Data on 16 OPCC staff working in the local area will be used, for the duration of the consultancy (estimated up to three months, of which several days will be dedicated to dealing with this data)

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 individuals concerned are all employed by the OPCC. It may not be possible to grant access to the data on a granular basis, and so the consultants will be required to access their "personnel record" as a whole. It is reasonable to conclude that aggregating data about terms and conditions is expected of an employer in order to ensure fairness. No children or vulnerable groups are involved and there are no known concerns.

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 benefits of this processing will be to: • Better understand the variety of terms and conditions under which OPCC staff are working • Identify opportunities to improve or standardise terms and conditions of employment • This will allow the organisation to ensure fairness and consistency in contracts

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?
It is proposed that prior to any work being undertaken: • All OPCC staff are briefed on the project, its aims and objectives and how it will benefit the organisation and themselves • All staff will be individually requested to grant access to their personnel record, clearly indicating what data will be used, and what other data may be seen as a result • Staff will be given the opportunity to opt-out of having their personal data used as part of the consultancy programme – and have the right to withdraw their consent at any time

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 bases are: - **Consent** will be sought from all personnel in order to ensure they understand the reasons for their personal data being used, and better engage with the programme of work - The OPCC has a **legitimate interest** in transferring the personal data from the force system to the OPCC system in order to fulfil its duty as an employer The outcome of the consultancy could also be served by means of interviewing staff and/or asking them to volunteer information to the consultants instead of granting direct access to their personnel system data. Access will only be granted on-site to vetted consultancy staff in order to minimise risks. The data subjects will be informed before, during and after the consultancy of progress and its outcomes. A Data Protection Officer will be available to address any concerns and staff will have the right to withdraw their consent at any time.

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
Loss, theft or disclosure of sensitive personal data	Possible	Severe	Medium
Inadvertent access to or viewing of some personal data unrelated to the project	Possible	Minimal	Low
Loss or theft of data during electronic transfer between systems	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
Loss, theft or disclosure of sensitive personal data	Only vetted staff allowed to access or process data	Reduced	Low	Yes
	Require data to be viewed on force networked terminals only	Reduced	Low	Yes
Inadvertent access to or viewing of some personal data unrelated to the project	Only vetted staff allowed to access or process data Require data to be viewed on force networked terminals only	Reduced	Low	Yes
Loss or theft of data during electronic transfer between systems	Ensure data is transferred over secure force network and no removable media is used	Reduced	Low	Yes

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:	Rachel Cook	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Michael Richmond OPPC DPO 14/8/2018	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Ensure all staff are given the right not to take part in the analysis part of the process, and that an explanation is given of why their data is being transferred to the OPCC. Ensure all contractors are vetted and only access and view data on force networked terminals. No personal data to be printed or transferred offsite in any way – only aggregated or depersonalised data. DPO approval to be sought for any depersonalised or anonymised data.		
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:	Mike Richmond	The DPO should also review ongoing compliance with DPIA