

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 OPCC, on behalf of the local Criminal Justice board wishes to better understand the local experience of the Criminal Justice System for victims of crime. This work is in response to a data request from the Ministry of Justice as part of the assurance work around the Victims Code of Practice (VCOP). An external agency, Agencia, have been contracted to deliver this work which comprises of three strands:

- 1: Collection of performance data from agencies: the Police, CPS, HMCTS, Victim Support and the National Probation Service.
- 2: Collection of anecdotal information about the local experience of delivering compliance with the VCOP.
- 3: Collection of qualitative data from victims of crime by means of survey, interview and online focus group

A DPIA has been identified due to the possibility that criminal offence data will be disclosed as part of this process, and because of the large scale of the processing, with 19,000 invitations sent out to people who have already agreed to receive communication from the OPCC.

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?

For each strand:

1: No personal data will be collected in this part of the process. There is an option to track cases from start to finish in the MOJ request, but we will instead be asking agencies to supply only aggregated data.

2: No personal data will be collected in this part of the process. Interview responses will not be attributed to agencies or respondents.

3: The surveys will be done in two parts: the first will be a survey asking for broad experiences of being a victim of crime, with responses given as numbers on a Likert scale and free text. Results will be aggregated and comments no attributed to specific respondents. The data will be captured on the My Community Alert system (which is shared with the force and subject to the police force's data protection regime) and supplied to the OPCC who will ensure no personal data is within it before handing it to Agencia to process.

The final questions of this response will seek respondents' permission to contact them for further discussions. This will be captured under the existing privacy policy for My Community Alert. Once contact details have been provided, the OPCC will contact the people on the list on behalf of Agencia to invite them to take part in the qualitative study. The study will be conducted by Agencia as our data processor and this will be made clear to participants. The data will be anonymized, as it will not be attributed to specific victims, although a risk remains that a victim could be identified due to them speaking about a very specific offence. If this is considered likely then a risk assessment will be completed and the data left out of the report.

Online focus groups may be conducted using the Delib system, in which all respondents will be anonymous and represented by an avatar. Should they disclose personal data voluntarily this will not be used without their permission. Telephone interviews will be conducted by Agencia staff, but they will not attribute responses to specific respondents.

Agencia, upon completion of their contract, will return all personal data to the OPCC and delete their copies of all source data. All personal data will be deleted by the OPCC either on request or a maximum six months after the report has been completed.

The full report will only be seen by OPCC staff and the Criminal Justice board, all of whom are senior representatives of criminal justice agencies. A summary may be made available to the public but no personal data will be included in either report.

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 in section 3 will include sufficient personal data to contact respondents who have consented for us to do so. It could include criminal offence data in the free text – though this will not be solicited. It will be retained for a maximum of six months from publication of the final report and no later than the end of 2020. All contact details will be deleted at that point. Respondents will be people from within the Humberside area who have consented to be contacted by the OPCC and further consented for us to contact them. This could be up to 19,000 people but is anticipated to be far fewer.

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 concerned have opted in to communications from the OPCC. There are no known children but there may be people considered vulnerable due to other factors. Vulnerability cannot be determined from the contact data in the My Community Alert System but may be identified later as part of the interviews/online focus groups.

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 processing will identify opportunities to improve local victims services and ensure that the Police and Crime Commissioner spends his funds appropriately. This will lead to a better experience for victim and potentially improve the effectiveness of criminal justice in the area.

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?

We will seek the views of individuals by only speaking to victims who have opted in to doing so, and by keeping them informed of how we will use their data at the point they are invited to take part in the qualitative part of the study.

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?

We will only collect enough personal information to contact respondents – email address or phone number plus their name. We will rely on the lawful basis of consent for this piece of work. All data will be handed to the OPCC at the end of the contract and reviewed for proportionality, with data being deleted where it is not required. Individuals are to be informed of how we will use their data and who we will share it with if they opt to take part in the study. The processor will be bound by contract to follow our requirements in this area.

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>Person discloses information in a free text box, revealing personal or criminal offence data where it was not expected. This could lead to them believing they had reported something to the police and not the OPCC.</p> <p>Personal data of respondents is lost or inadvertently breached by Agencia</p>	<p>Remote, possible or probable Possible</p>	<p>Minimal, significant or severe Minimum</p>	<p>Low, medium or high Low</p>
		Possible	Significant

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
Personal data of respondents is lost or inadvertently breached by Agencia	Agencia contracted to follow our data protection rules. Clear privacy policy supplied when people are invited to focus groups so they understand who is handling their data.	Reduced Eliminated reduced accepted	Low medium high	Yes/no Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Robbie Walker-Brown	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Robbie Walker-Brown	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Michael Richmond	DPO should advise on compliance, step 6 measures and whether processing can proceed
<p>Summary of DPO advice:</p> <p>Ensure that a privacy policy is supplied with the invitation to secondary interviews, other personal data is already covered by the My Community Alert force DP regime, which we accept.</p>		
DPO advice accepted or overruled by:	Robbie Walker-Brown	If overruled, you must explain your reasons
<p>Comments:</p>		
Consultation responses reviewed by:	N/A	If your decision departs from individuals' views, you must explain your reasons
<p>Comments:</p>		

This DPIA will kept under review by:	Michael Richmondr	The DPO should also review ongoing compliance with DPIA
--------------------------------------	-------------------	---