Ministry of Defence Police

Data Protection Impact Assessment (DPIA)

Name of System or Project:	
Information Asset Owner or Project Leader:	
Date of DPIA Sign Off:	

This DPIA will be reviewed annually or whenever there is a significant change which may impact on the processing of information within the system/project.

The review will be led by the Information Asset Owner or Project Leader.

What is a DPIA?

A DPIA is necessary if we plan to systematically and comprehensively analyse our processing and helps us to identify and minimise data protection risks. They consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm to individuals or to society at large, whether it is physical, material or non-material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping us to demonstrate accountability and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations.

It's important to embed DPIAs into our organisational processes and ensure the outcome can influence our plans. A DPIA is not a one-off exercise but should be seen as an ongoing process regularly reviewed.

When do we need a DPIA?

We will do a DPIA before we begin any type of processing which is "likely to result in a high risk". This means that although we have not yet assessed the actual level of risk we need to screen for factors that suggest potential for widespread or serious impact on individuals.

We should also think carefully about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data.

How do I conduct a DPIA?

The need for a DPIA can be established by answering the Screening Questions below.

If the answers to all Screening Questions are NO, then no further assessments are required and proceed straight to STEP 7 for Sign Off.

If the answer to any Screening Question is YES, then complete STEP 1 - 7.

DPIA Screening Questions

Does the system or project plan to:

(Delete Yes/No as appropriate)

(a)	Use systematic and extensive profiling or automated decision-making to make significant decisions about people	YES/NO
(b)	Process special category data or criminal offence data on a large scale	**YES/NO**
(c)	Systematically monitor a publicly accessible place on a large scale	**YES/NO**
(d)	Use new technologies	**YES/NO**
(e)	Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit	**YES/NO**
(f)	Carry out profiling on a large scale	**YES/NO**
(g)	Process biometric or genetic data	**YES/NO**
(h)	Combine, compare or match data from multiple sources	**YES/NO**
(i)	Process personal data without providing a privacy notice directly to the individual	**YES/NO**
(j)	Process personal data in a way which involves tracking individuals' online or offline location or behaviour	**YES/NO**
(k)	Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them	**YES/NO**
(l)	Process personal data which could result in a risk of physical harm in the event of a security breach	**YES/NO**

Next Steps

If the answers to ALL of the above Screening Questions are NO, proceed straight to STEP 7 for Sign Off.

If any of the answers to the Screening Questions are YES, complete STEPS 1-7.

Step 1: Identify the need for a DPIA

Explain broadly what the system or 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 from the Screening Questions why you identified the need for a DPIA.

2.1. Describe the nature of the processing: For example, 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?

2.2. Describe the scope of the processing: For example, 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?

2.3. Describe the context of the processing: For example, 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)?

2.4. Describe the purposes of the processing: For example, 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?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: For example, 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?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: For example, 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?

Step 5: Identify and assess risks

Using the table below, describe the source of the risks and nature of their impact on individuals associated with your system or project in Column (a). Then assess the likelihood of harm occurring (b), the severity of that harm (c), and the overall risk (d) using the risk matrix opposite.

		SEVERITY OF HARM (c)			
		Acceptable	Tolerable	Undesirable	Intolerable
LIKELIHOOD OF HARM (b)	Highly Improbable <10% Risk is highly unlikely to occur	VERY LOW	LOW	MEDIUM	HIGH
	Improbable i.e. <25% Risk is unlikely to occur	LOW	MEDIUM	MEDIUM	HIGH
	Possible i.e. >25% Risk may occur	LOW	MEDIUM	HIGH	HIGH
	Probable i.e. >50% Risk is more likely to occur	LOW	MEDIUM	HIGH	VERY HIGH
	Highly Probable (i.e. >75%) Risk will almost certainly occur	LOW	MEDIUM	VERY HIGH	VERY HIGH

(a) Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	(b) Likelihood of harm	(c) Severity of harm	(d) Overall risk
(1) Risk breaching Principle 1 (Lawfulness, fairness and transparency) in that data subjects may feel their personal data is collected unfairly. **(2) Risk breaching Principle 2 (Purpose limitation) in that data subjects may feel that the processing of their personal data may become a disproportionate intrusion of their privacy.** **(3) Risk breaching Principle 3 (Data minimisation) in that data subjects may consider the amount of information being obtained is excessive.** **(4) Risk breaching Principle 4 (Accuracy) in that data subjects may have concerns regarding the accuracy of their personal data.** **(5) Risk breaching Principle 5 (Storage limitation) in that data subjects may have concerns regarding the length of time their personal data is being held and affecting their right to privacy.** **(6) Risk breaching Principle 6 (Integrity and confidentiality) in that data subjects may have concerns regarding the security of their data.** **(7) Risk breaching Principle 7 (Accountability) in that data subjects may have concerns regarding the application of their statutory information rights under the DPA and FOIA.**			

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**
1				
2				

3 4 5 6				

7				

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	**Project Manager**	*Integrate actions back into project plan, with date and responsibility for completion*
Residual risks approved by:		*If accepting any residual high risk, consult the ICO before going ahead*
DPA advice provided by:	**MDP-Sec-DPA**	*DPA should advise on compliance, step 6 measures and whether processing can proceed*
Summary of DPA advice:		
DPA advice accepted or overruled by:	**Project Manager**	*If overruled, you must explain your reasons*
Comments:		
Consultation responses reviewed by:	**Project Manager**	*If your decision departs from individuals' views, you must explain your reasons*
Comments:		
This DPIA will kept under review by:	**Force Information Manager**	*The DPA should also review ongoing compliance with DPIA*

DPIA Signed off by:	**(name)**	**(date)**