



Ministry of Defence Police

Freedom of Information Manager

Room 126 Building 1070

MDP Wethersfield

Braintree CM7 4AZ

United Kingdom

Telephone: +44 (0)1371 85[REDACTED]

E-mail: MDP-FOI-DP@mod.gov.uk

Our Ref: eCase: FOI2018/11368 RFI:276/18

Date: 26 September 2018

[REDACTED]
[REDACTED]
[REDACTED]
Dear [REDACTED]

FREEDOM OF INFORMATION ACT 2000: MINISTRY OF DEFENCE POLICE: DATA PROTECTION DOCUMENTS

I refer to your e-mail dated 04 September 2018, which was acknowledged on the 05 September 2018.

We are treating your e-mail as a request for information in accordance with the Freedom of Information Act 2000 (FOIA 2000).

In your e-mail you requested the following information:

“I would like to obtain copies of any forms or templates used in relation to compliance with data protection law by the MOD Police ideally in PDF format. Examples of such documents which may be held by the authority include:

- Data Protection Policy;
- IT Acceptable Use Policy;
- Procedures applicable to data protection;
- Blank templates such as:
- Subject Access Request Form;
- Breach Notification Form;
- DPIA;
- Standard Data Processing Agreement;”

A search for information has now been completed by the Ministry of Defence Police and I can confirm that we do hold information in scope of your request.

The policies the Ministry of Defence Police follow are those laid down by the Ministry of Defence.

The MDP privacy notice can be found on the link below.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708924/Ministry_of_Defence_Police_Information_Charter.pdf

Please also see the attached documentation.

If you have any queries regarding the content of this letter, please contact this office in the first instance.

If you wish to complain about the handling of your request, or the content of this response, you can request an independent internal review by contacting the Information Rights Compliance team, Ground Floor, MOD Main Building, Whitehall, SW1A 2HB (e-mail CIO-FOI-IR@mod.gov.uk). Please note that any request for an internal review should be made within 40 working days of the date of this response.

If you remain dissatisfied following an internal review, you may raise your complaint directly to the Information Commissioner under the provisions of Section 50 of the Freedom of Information Act. Please note that the Information Commissioner will not normally investigate your case until the MOD internal review process has been completed. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Further details of the role and powers of the Information Commissioner can be found on the Commissioner's website at <https://ico.org.uk/>.

Yours sincerely

MDP Sec Freedom of Information Office



Ministry of Defence Police

Request to external organisation for the disclosure of personal data to the Police

Under Schedule 2 Part 1 Paragraph 2 of the Data Protection Act 2018 and GDPR Article 6(1)(d)

To:

Position (where known): [Click or tap here to enter their position in their organisation.](#)

Organisation: [Click or tap here to enter name of their organisation.](#)

Address: [Click or tap here to enter address of their organisation.](#)

I am making enquiries which are concerned with:

- The prevention or detection of crime*
- The prosecution or apprehension of offenders*
- Protecting the vital interests of a person*

I confirm that the personal data requested below is needed for the purposes indicated above and a failure to provide that information will be likely to prejudice those matters.

I confirm that the individual(s) whose personal data is sought should not be informed of this request as to do so would be likely to prejudice the matters described above.

**Check mark as is appropriate*

Information required:

[Click or tap here to enter text setting out what information is required.](#)

Police Reference:

[Click or tap here to enter Crime Reference No., Case File No. etc. where necessary](#)

From:

Rank/Number/Name: [Click or tap here to enter details of person completing form.](#)

Station: [Click or tap here to enter details of station where you are based.](#)

Date/Time: [Click or tap here to enter date and time of completion.](#)

Telephone Number(s): [Click or tap here to enter your telephone number\(s\).](#)

Email address: [Click or tap here to enter your official police email address.](#)

Signature*:

Counter Signature:*

Rank/Number/Name: [Click or tap here to enter details of person providing counter signature.](#)

**as required by recipient*

Please see Guidance Notes on following page

Explanatory Note

This form replaces the Section 29(3) Form which has become redundant by virtue of new data protection legislation. It is used by the police as a means of making a formal request to other organisations for personal data where disclosure is necessary for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders. It places no compulsion on the recipient to disclose the information, but should provide necessary reassurance that a disclosure for these purposes is appropriate and in compliance with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Crime and Taxation - The GDPR regulates the processing of personal data where it is done so for non-Law Enforcement purposes. Article 23 of the GDPR permitted the UK Parliament to create, via legislation, exemptions from particular elements within the GDPR which would otherwise compromise the public interest.

Consequently Parliament used the Data Protection Act 2018 to set out exemptions from the GDPR which apply in some circumstances. They mean that some of the data protection principles and subject rights within the GDPR do not apply at all or are restricted when personal data is used or disclosed for particular purposes.

The most relevant exemption for Law Enforcement is that within the Data Protection Act 2018 at Schedule 2 Part 1 Paragraph 2 (Crime & taxation: general). This applies where personal data is disclosed by an organisation subject to the GDPR to the police for the purposes of *the prevention or detection of crime or the apprehension or prosecution of offenders*.

It restricts the application of the GDPR data protection principles and subject rights (as listed in the Data Protection Act 2018 at Schedule 2 Part 1 Paragraph 1) to the extent that the application of those provisions would be likely to prejudice *the prevention or detection of crime or the apprehension or prosecution of offenders*.

In effect the exemption means that an organisation can provide personal data to the police where necessary for the prevention or detection of crime or the apprehension or prosecution of offenders without fear of breaching the GDPR or Data Protection Act 2018.

Vital Interests – GDPR Article 6(1)(d) provides a lawful basis for organisations to disclose personal data to the police where the disclosure *is necessary in order to protect the vital interests of the data subject or of another natural person*.

Further guidance on the use of this form may be obtained from the force Data Protection Officer.

Completion Guidance

Police officers or staff completing this form should type and tab between the fields on the form. The information required field should provide the recipient with sufficient information to allow them to locate the information sought. Where a signature and/or counter signature are required the form will need to be printed off and signed manually. Some organisations may require a counter signature to be added to the form. Normally this should be the supervisor or line manager of the person completing the form, but may be a higher rank if reasonably required by the recipient.

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

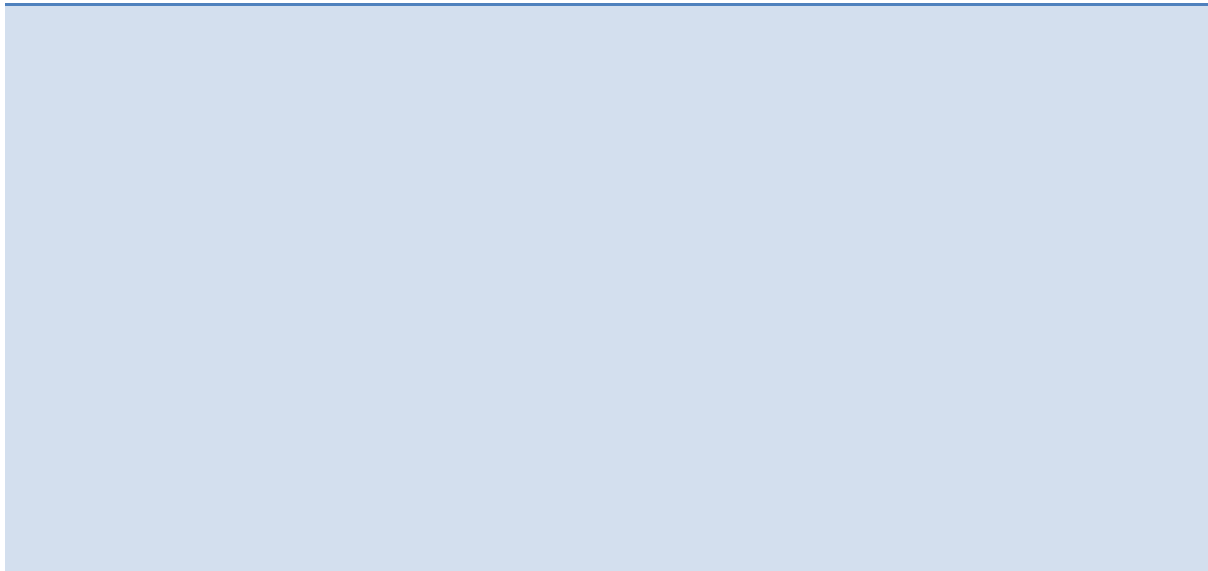
If the answers to ALL of the above Screening Questions are NO, proceed straight to STEP 7 for Sign Off.

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

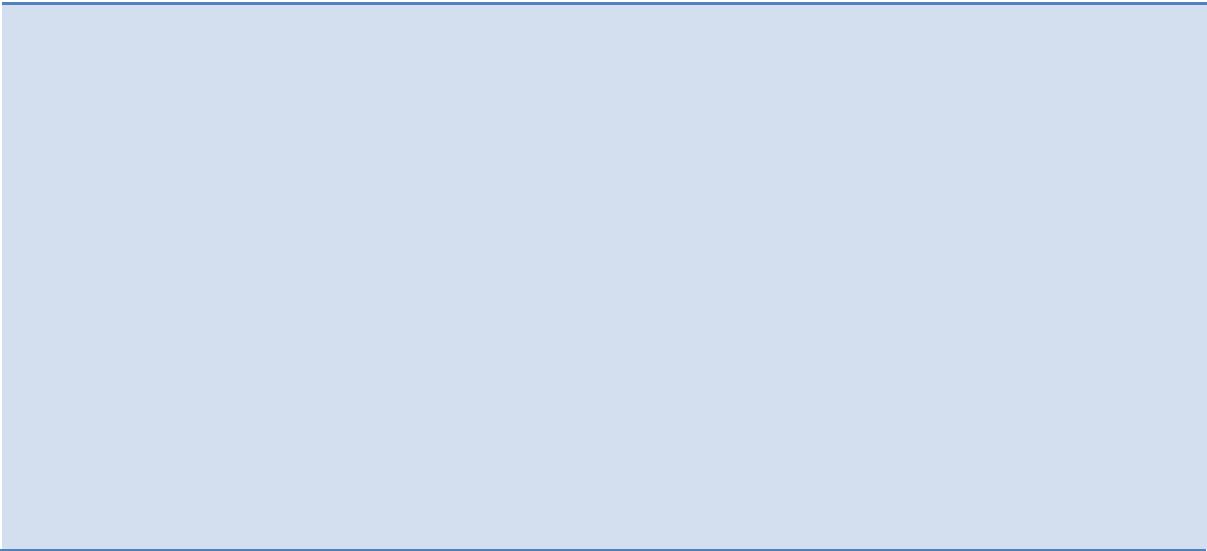
Step 1: Identify the need for a DPIA

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.

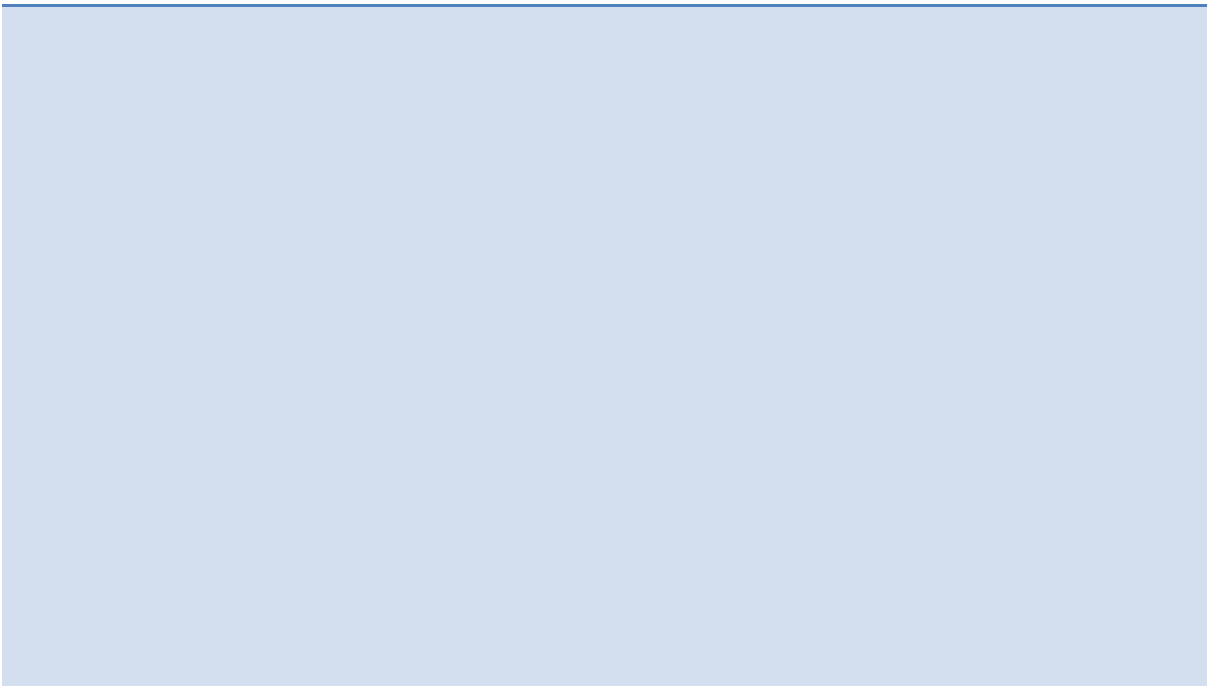
2.1. Describe the nature of the processing: For example, how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?



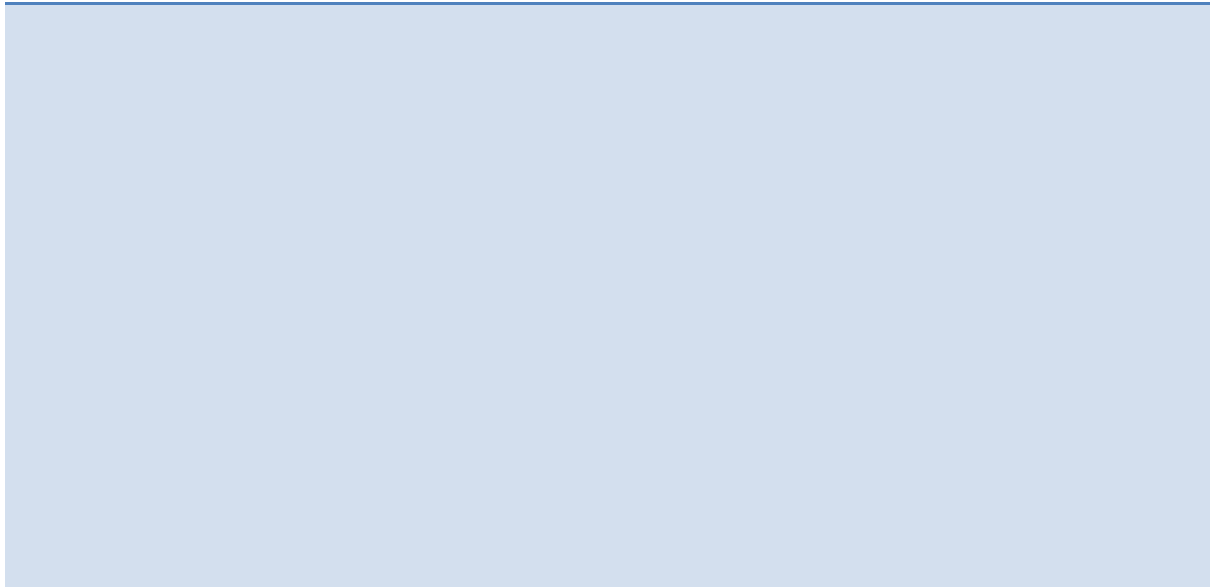
2.2. Describe the scope of the processing: For example, what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it 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)?

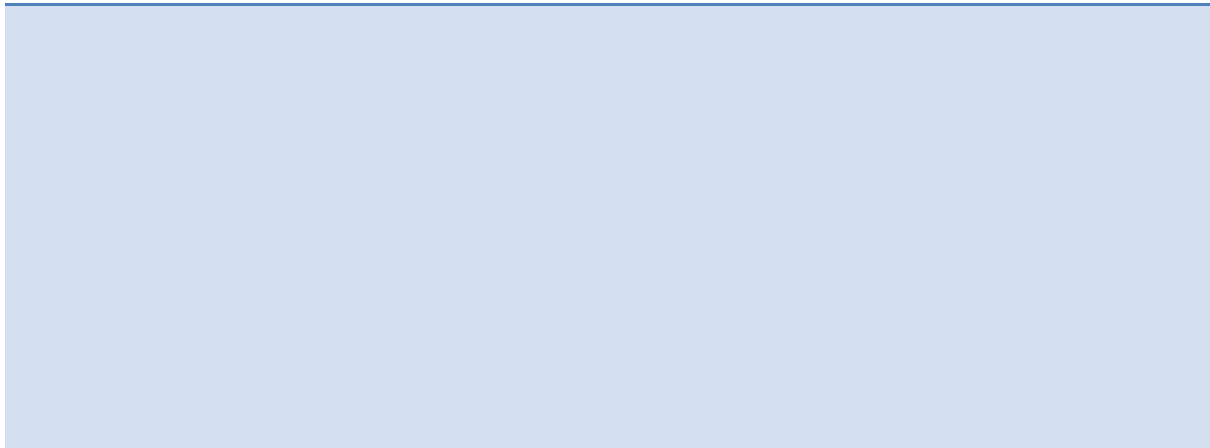


2.4. Describe the purposes of the processing: For example, what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?



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)	<u>Highly Improbable</u> <10% Risk is highly unlikely to occur	VERY LOW	LOW	MEDIUM	HIGH
	<u>Improbable</u> i.e. <25% Risk is unlikely to occur	LOW	MEDIUM	MEDIUM	HIGH
	<u>Possible</u> i.e. >25% Risk may occur	LOW	MEDIUM	HIGH	HIGH
	<u>Probable</u> i.e. >50% Risk is more likely to occur	LOW	MEDIUM	HIGH	VERY HIGH
	<u>Highly Probable</u> (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
<p>(1) Risk breaching Principle 1 (Lawfulness, fairness and transparency) in that data subjects may feel their personal data is collected unfairly.</p> <p>(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.</p> <p>(3) Risk breaching Principle 3 (Data minimisation) in that data subjects may consider the amount of information being obtained is excessive.</p> <p>(4) Risk breaching Principle 4 (Accuracy) in that data subjects may have concerns regarding the accuracy of their personal data.</p> <p>(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.</p> <p>(6) Risk breaching Principle 6 (Integrity and confidentiality) in that data subjects may have concerns regarding the security of their data.</p> <p>(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.</p>			

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



Data Protection Act 2018 Subject Access Request (SAR) Form



Please note, this form should only be used to request information about a living individual.

Please complete in **BLACK** in **BLOCK CAPITAL LETTERS** in the boxes.

- I am the Data Subject (The person the information is about): **OR**
- I am acting on behalf of the Data Subject: **Complete Part 2, 3 and 4**

If you are seeking information on behalf of someone who is unable to act for themselves, you must explain your relationship with that person, what information you require and why it is required. Please note that information relating to someone else will not be disclosed without the data subject's written consent or an appropriate Court Order or Power of Attorney. Accordingly I enclose:

The Data Subject's written consent to disclosure of the information requested at Part 3:

A Court Order (e.g. Power of Attorney) permitting release of the information requested at Part 3:

Proof of identity for the Data Subject and proof of identity for myself (see Part 4 for details of what is acceptable identification)

My relationship to the data subject is:
(Please specify e.g. Doctor/Solicitor/Spouse/Civil Partner/Father/Mother/Brother/Sister etc)

Part 1 – Data Subject Personal Details

Surname:		Full Forename(s):		Title:	
Surname while Serving (if different):		Service/Staff No:		Rank/Grade:	
Date of Birth:		National Insurance Number:			
Please provide your daytime telephone number or e-mail in case we need to contact you about your request:					
Daytime Tel. No:	E-mail address:				
Postal Address:					
Postcode:	County:				
MOD Service	Royal Navy: <input type="checkbox"/>	Civilian: <input type="checkbox"/>	Other: <input type="checkbox"/> Please provide details:		
	Army: <input type="checkbox"/>				
	Royal Air Force: <input type="checkbox"/>				
	Home Guard (HG): <input type="checkbox"/>	Date(s) of Joining:		Date(s) of Leaving:	
	County served in (HG only):				

Part 2 – Enquirer's Details (if different from above).

If seeking information on behalf of someone else please also provide your full name. Please also provide the address that you want the information sent to plus your daytime telephone number in case we need to speak to you to discuss the request

Surname:		Full Forename(s):		Title:	
Postal Address:					
Postcode:	Country:				
Daytime Tetl No:					

Part 3 – Information Requested

State clearly the information you require, with dates where known e.g. *my medical records while serving at HMS Centurion 1990-1993*

Please provide as much information as possible to assist us in locating your data

--	--



MOD will use the information provided for the purpose of locating the information requested and it will kept securely for a minimum of 2 years in case of further enquiries from you. We recommend that you read the [Personal Information Charter](#) and the [MOD's Privacy Notice](#) in full as they provide more detail on how we manage personal data.

Part 4 – Declaration

Verification of identity is required before your request can be processed. If you have changed your name since your service then proof of this name change will also be required in the form of marriage licence/deed poll certificate etc.

Please provide:

- [1] a copy of your Photocard Driver's Licence **OR**
- [2] your current Passport showing photo and signature **AND** a copy of a recent domestic utility bill or official correspondence confirming current home address dated within the last three months.

I enclose as verification of identity a photocopy of my:	Driving Licence: <input type="checkbox"/>	Passport: <input type="checkbox"/>	Utility Bill: <input type="checkbox"/>	Other: <input type="checkbox"/>
--	---	------------------------------------	--	---------------------------------

I declare that, to the best of my knowledge, the information I have provided on this form is correct.

Signature:		Name in Capitals:	
		Date:	

Official Sensitive Personal (When completed)

PART 5 – What to do Next

If you are the Data Subject and still serving in the Armed Forces, the request should be sent to the Data Protection Adviser at the Current Unit Admin Office or Unit Medical Centre.

If the Data Subject is discharged, or is one of the other categories of requestor, the request should be sent to one of the following addresses together with proof of identity (plus written consent and/or court order/Power of Attorney if you are acting on behalf of the data subject). Requests by email or other means (i.e. social media) are acceptable but must be accompanied by the relevant documentation.

If you served in the following:	Send your request to this address:
Royal Navy or Royal Marines:	RN Disclosure Cell, Mail Point 1.3, Navy Command Headquarters, Leach Building, Whale Island, Portsmouth, Hampshire, PO2 8BY NAVYSEC-DISCELLMAILBOX@mod.gov.uk
Royal Navy Medical Records	RN Service Leavers, Institute of Naval Medicine, Crescent Road, Alverstoke, PO12 2DL NavyINM-RNServiceLeavers@mod.gov.uk
Army or Home Guard:	Army Personnel Centre, Disclosures 2, Mail point 535, Kentigern House, 65 Brown Street, Glasgow, G2 8EX apc-sp-disclosures2@mod.uk
For Army Medical Records (for discharged personnel only):	Army Personnel Centre, Disclosures 3, Mail point 525, Kentigern House, 65 Brown Street, Glasgow, G2 8EX apc-sp-disclosures3@mod.uk
RFA Seafarers:	RFA Pers Ops, Room 13, Mail Point G1, West Battery, Whale Island, Portsmouth, PO2 8DX
Royal Air Force:	RAF Disclosures, Room 15, Trenchard Hall, RAF Cranwell, Sleaford, Lincolnshire, NG34 8HB air-cospers-disclosures@mod.gov.uk
DECA:	Data Protection Adviser, HRBP, DECA Sealand, Welsh Road, Deeside, Flintshire, CH5 2LS
Service Personnel /Veterans (AFPS, AFCS, WPS only):	Defence Business Services Mail and Scanning Hub, PO Box 38, Cheadle Hulme, Cheshire SK8 7NU PeopleServices@dbs.mod.uk
MoD Civilians:	Defence Business Services Mail and Scanning Hub, PO Box 38, Cheadle Hulme, Cheshire SK8 7NU PeopleServices@dbs.mod.uk
DSTL:	DSTL SDPO, i-Sat B, G01, Bldg 5, DSTL, Porton Down, Salisbury, Wilts, SP4 0JQ
Hydrographic Office:	DPA Focal Point, UK Hydrographic Office, Admiralty Way, Taunton, Somerset, TA1 2DN
Ministry of Defence Police:	Data Protection Adviser, Bldg 1070, MDP Wethersfield, Braintree, Essex, CM7 4AZ
Defence Infrastructure Organisation	Data Protection Adviser, Chief Information Office, Defence Infrastructure Organisation Kingston Road, Sutton Coldfield, B75 7RL DIOCIO-DPO@mod.gov.uk
Others e.g. if you are a member of the public	MOD HQ SAR Coordinator, G.M. Main Building, Horse Guards Avenue, Whitehall, London SW1A 2HB
If you believe you have been subject to hazardous materials:	Please complete the Special Subject Access Request form instead

Part 6 – For MOD Use Only

Actioned By: <i>(Name in Capitals)</i>		Date Received:		SAR Reference No:	
Signature:		Date Responded:		Disposal Date:	

Part 7: Final Checklist

Have you included everything:

Data Subject's personal details and details of the Data Subject's service:	
Data Subject's Postal Address:	
Your address (if different):	
Have you completed Part 3 of the form:	
Proof of Identity (Data Subject):	
Proof of Identity (if you are acting on behalf of someone else):	
Power of Attorney, Court Order or consent of Data Subject (if appropriate):	
Proof of Change of Name (if appropriate):	
Have you signed the form:	