Defence Electronics &
Components Agency

Defence Electronics & Components Agency
Building 15
Welsh Road
Deeside
Flintshire
CH5 2LS

Telephone: [redacted]
Email: foifocalpoint@deca.mod.uk

Ref: FOI2019/02286
19 March 2019

[redacted]

Dear [redacted]

I am writing in response to your email dated 20 February 2019. I am treating your correspondence as a request for information under the Freedom of Information Act 2000 (FOIA).

Please provide me with a copy of your full GDPR Data Protection Impact Assessment (DPIA) questionnaire/assessment/template. It can be blank with no responses included so there is no concern with any sensitive data being released. This request should include any preliminary questions or any questions/mechanism for determining if a DPIA is required to be completed.

These assessments are required under Article 35 of GDPR

In response to your queries, I have completed a search for the information within the Defence Electronics & Components Agency (DECA), and I can confirm that **we do hold information in scope of your request** and information is included at Annex A

If you are not satisfied with this response or you wish to complain about any aspect of the handling of your request, then you should contact me in the first instance. If informal resolution is not possible and you are still dissatisfied then you may apply for an independent internal review by contacting the Information Rights Compliance team, Ground Floor, MOD Main Building, Whitehall, SW1A 2HB or by e-mailing CIO-FOI-IR@mod.uk. Please note that any request for an internal review must be made within 40 working days of the date on which the attempt to reach informal resolution has ended.

If you remain dissatisfied following an internal review, you may take your complaint to the Information Commissioner under the provisions of Section 50 of the Freedom of Information Act. Please note that the Information Commissioner will not investigate your case until the MOD internal review process is complete. You can find further details of the role and powers of the Information Commissioner on the Commissioner's website.

Regards

[redacted]
DECA FOI

Ministry
of Defence

MOD Pre-DPIA & DPIA Workbook Introduction

Version 1 - 31/01/2019

Purpose

This is the official MOD Pre-DPIA and DPIA Workbook and must be used by all MOD personnel that process data. This workbook is designed to help MOD determine if your processing activity needs to be risk assessed via a Data Protection Impact Assessment, and conduct one, if it is. The workbook is aimed at Information Asset Custodians (IAC) or an equivalent role.

What is a Data Protection Impact Assessment?

A Data Protection Impact Assessment (DPIA) is a process to help us identify and minimise the data protection risks of a project or processing activity. A DPIA is legally required if the activity in question will likely result in a high risk to peoples rights and freedoms.

Instructions

If your system, project or process involves the processing of *any* data, please download this workbook and complete Part 1A and follow the instructions. These can be found throughout in dark grey boxes. Please ensure you enable the workbook so you can use the drop-down list and checkbox features.

The questions in this workbook combine those set out by the Information Commissioner's Office and MOD policy to meet our legal obligations. Answer each question as fully, accurately and transparently as you can, as the information you supply will be used the inform this assessment. Please cross-refer to the guidance in the far right column to help you answer the questions. If you need further guidance, please consult your Data Protection Advisor (DPA) or the MOD Data Protection Officer's Team (cio-dpa@mod.gov.uk.)

This form will be reviewed outside your business unit and may be reviewed outside your Top Level Budget, Arms-Length Body, or outside the MOD. Therefore, please expand all acronyms or abbreviations. Failure to do so will delay the completion of the process, as the form will be returned for clarification.

Record of outcome

Once you have completed the workbook, please save it in an appropriate area using the correct naming convention and security classification. The security classification must reflect the information supplied, as such, you may need to alter the security classfication at the top of each page. This workbook must be reviewed whenever the processing activity you have risk-assessed changes, or if there are no changes, annually. It is best practice to save one version of this workbook in one location and provide access to those necessary for its completion and review.

Part 1
Pre-DPIA & DPIA Workbook details

Part 1A - Basic details		**Response**
1	Which Top Level Budget, High Level Budget or Arms-Length Body are you from?	
2	What is your domain, operating centre or business unit called?	
3	What is your name?	
4	What is your job title?	
5	What is your email address?	
6	What is the name of the system, process or project? What is it and what does it do?	
8	Do you plan to process any personal data?	
If you are not going to process any personal data, go straight to Part 3. A DPIA will not be required.		

Part 1B - Personal data		**Response**
1	Please state all the types of personal data you are going to process.	
2	You **must** have a lawful basis to legally process personal data. Which of the following reasons best describes why you are processing personal data?	
If you cannot identify a suitable reason at Part 1B, question 2 (above), seek advice from your Data Protection Advisor before you process any personal data.		
3	Why exactly are you processing this data? What are the benefits / expected outputs of using personal data?	
4	You must have an additional lawful reason **if** you want to process 'special category' personal data. **If** you are processing special category data, please explain why:	

If you are processing special category data and cannot identify a suitable condition at Part 1B, question 4 (above), seek advice from your Data Protection Advisor before you process any special category data.		
5	Why exactly are you processing this data? What are the benefits / expected outputs of using special category data? (if applicable)	
6	Is there any other way you could achieve the same outcome *without* processing personal data / special category personal data?	
7	What IT systems / applications will you be using to conduct this processing? (if any)	
8	If you are not using IT systems / applications, how will you process / hold the information?	
9	Who are you sharing the data with? (e.g. within MOD / other government departments / externally)	
10	If you are sharing this data outside the MOD, do you have a contract or data sharing agreement in place? If not, why not?	

Part 1C - Other details		**Response**
1	Who is your Data Protection Advisor (DPA)?	
2	Who is the Information Asset Owner (IAO)?	
3	Who is the Senior Information Risk Officer (SIRO)?	
4	Please name any additional advisors e.g. accreditors, information security, commercial that you will consult regarding this system, process or project (if applicable)	

Part 2
Pre-DPIA

Part 2A - High risk questions		**Yes/No**	**Comments** (if applicable)
Will this processing involve:			
5	Processing over 10,000 pieces of personal data, of any kind?		
1	Processing over 1,000 pieces of special category data?		
2	Using special category data to decide if someone can access a service, opportunity or benefit?		
3	Processing over 1,000 personal records concerning criminal activity or offences?		
4	Processing any personal data about the protected population?		
6	Processing any children's personal data for marketing purposes / so you can offer them online services?		
7	Processing personal data that could result in physical harm if it was disclosed, accessed, lost, altered or destroyed without authorisation?		
8	Processing personal information that is **not** covered by the MOD Privacy Notice or by your own bespoke privacy notice? If yes, add comment explaining why		
9	Combining, comparing or matching data from different sources or systems?		
10	Making automated decisions?		
11	Processing personal data gained by tracking virtual location or behaviour?		
12	Processing personal data gained by tracking physical location or behaviour?		
13	Using technologies that (as far as you're aware) have not been used:		

Part 2B - Potential risk questions	**Yes/No**	**Comments** (if applicable)
If you don't know if the answer is 'yes' or 'no', answer 'yes' and add more information in the comments column.		
Will this processing involve:		

1	Collecting personal data that is currently not held by the MOD?		
2	Using personal data already held by the MOD, but for a new reason?		
3	Processing personal data on a new asset / system / device? *(If yes, please ensure you **record this** on the information asset register - see guidance)*		
4	Processing any security vetting data?		
5	Processing ***any*** special category data?		
6	Processing ***any*** personal information about children or vulnerable adults?	No	
7	Processing personal data covering more than one TLB and / or Arms-Length Body?		
8	Processing any biometric or genetic data?		
9	Processing any personal data for national security / intelligence / law enforcement purposes?		
10	Using personal information to evaluate or score the individuals concerned?		
11	Giving parties outside MOD that previously did not have access to the data, access now? If yes, who?		
12	Processing personal data outside the UK?		*Please enter country / countries*
13	Processing personal data that might cause MOD serious reputational damage if it were to be unlawfully disclosed or accessed, lost, altered or destroyed?		

Part 3
Pre-DPIA Outcome

Part 3A - Declaration						
1	Have Parts 1 and 2 been completed as per current MOD instructions?					
2	Signature		Email		Date	

Part 3B - Outcome (completed by DPA)						
1	Is a DPIA required?					
2	a) If **no,** why - and are any remedial actions are required?					
	b) Has the IAO agreed to enforce the actions above?					
3	If **yes,** which elements mean a DPIA must be completed?					
4	**DPA Name**	Alex Bath	**Email**	alex.bath100@mod.gov.uk	**Date**	31/01/2019

If a DPIA is required, please proceed to straight to Part 4. If in doubt, please complete the full DPIA at Part 4 and sign it off at Part 5.

Part 3C - Sign-off (if DPIA is not required)						
1	**IAO approved**	*Full name*	**Email**		**Date**	
2	**SIRO, PSYA approved - if required**	*Full name*	**Email**		**Date**	

Part 4
DPIA

Part 4A - The data		Response
1	How will the data be collected?	
2	How many pieces of personal data will be collected / processed overall?	
3	How will you ensure you only collect / process the personal data that you strictly need?	
4	How often will this data be refreshed, to ensure it is kept up-to-date?	
5	If the data will shared, how will it be shared / transferred?	
6	If the data is being transferred internationally (to a person / body based outside the UK), what safeguards will you put in place? (e.g. a contract, a data sharing agreement, other?)	
7	How will you ensure the data isn't unlawfully accessed / shared with anyone it doesn't need to be?	
8	How long is the personal data going to be kept for?	
9	How will the data be disposed of when it is no longer need it?	

Part 4B - Those identified by the data		Response
1	Approximately how many people are going to have their data processed?	
2	What categories do the individuals fall into? (tick all that apply)	
		□ They are non-MOD crown servants
		□ They are contractors
		□ They are children (under 13 yrs.) / vulnerable adults
		□ They are other members of the general public

3	What effect could holding or processing this information have on the individuals? Are there likely to be negative consequences for the individual, directly or indirectly? (e.g. physical, emotional or material harm)	
4	What control will the individuals have over their data? (tick all that apply)	□ They will be informed about this processing activity □ They can ask to have a copy of the data you hold □ They can ask the data to be rectified or completed if it's wrong □ They can ask any automated decisions to be conducted by a person instead □ They can ask us to stop / restrict processing their data □ They can ask the data to be processed somewhere else
5	What information is going to be made available to the individuals about this processing activity, and how will they be made aware of it?	□
6	Consider the reason you gave for processing their data at Part 1B, questions 3 and 5. Do you think they would reasonably expect their data to be processed for the reason described?	
7	Are there current issues of public concern that should be factored in?	N/A

Part 4C - Consultation process		**Response**
1	Which (if any) internal / external parties have been consulted about this processing?	N/A
2	What were their findings / views did they express? (if applicable)	N/A
3	How have their findings been implemented? If not, what were the reasons for not doing so?	N/A
4	If there has been no consultation, please explain why.	N/A

Part 4D - Risk management		**Response**

When reviewing the overall risk, please consider the answers above in conjunction with the answers given in Part 1, 2 and 3.		
1	If the personal data was accidentally (or intentionally and ***without*** authorisation) accessed, shared, changed, lost or destroyed, what impact could that have on the individuals or MOD business?	
2	What organisational and technological security measures are in place to prevent the above from happening?	
3	What risks to the individuals privacy rights and freedoms have been identified?	
4	**If** any privacy risks have been identified, refer to each risk above and consider what you **could** do to address the risk.	
5	**If** any privacy risks have been identified, **will** all the mitigations above be applied? If not, why not?	
6	Further to question 5, are there still any privacy risks left unaddressed? If so, what are they, and why are these risks are acceptable?	N/A
7	If this processing activity is going to be added to a risk register, please specify which register and enter a risk reference number.	

Part 5
DPIA Outcome

Part 5A - Declaration						
1	Have Parts 1, 2, 3 and 4 been completed as per current MOD instructions?					
2	Signature		Email		Date	

Part 5B - (completed by DPA)						
1	DPA comments					
2	**Name**		**Email**		**Date**	

Part 5C - Data Protection Officer consultation (completed by the MOD's Data Protection Officer or the Data Protection Officer's Team)						
1	DPO / DPO Team advice					
2	**Name**	*Full name*	**Email**		**Date**	
3	Advice from the Information Commissioner's Office (if applicable)					

Part 5D - Sign off (question 1 completed by DPA)						
1	DPO / ICO advice accepted? (if not, please explain why)					
2	**IAO approved**	*Full name*	**Email**		**Date**	
3	**SIRO approved**	*Full name*	**Email**		**Date**	

Part 5E - Review (completed by DPA)		
1	Date of next review	

DPA to submit or share signed copy of form to MOD's DPO Team (cio-dpa@mod.gov.uk) for inclusion in central records.

Pre-DPIA & DPIA Workbook Definitions

Personal data

Personal data is information that identifies a living individual, ***either on its own or in combination*** with other information. Personal data may include factors specific to the physical, physiological, genetic, mental, economic, culture or social identity of that person.

Non-exhaustive examples include: names (first or last); telephone number (work or personal); postcode / address (work or personal); email address (work or personal); internet protocol (IP) address; age; date of birth; gender; nationality; photograph; national insurance number; passport number; CCTV; organisation; branch or trade; rank; service number; staff number; performance appraisals; record of service; security clearance; criminal offence data; medical information; welfare information; pay, banking, financial details or credit card information; tax, benefit or pension records; welfare information; next-of-kin details; driving licence; education and or qualifications; course date; physical location; destination of travel, etc.

Processing

Processing includes collecting, storing, accessing, using, recording, destroying - or any other operation performed on personal data. Processing may be conducted by manual or automated means.

Special category data

Special category data concerns:

* race or ethnic origin;
* political, religious or philosophical beliefs;
* trade union membership;
* physical or mental health;
* sexual orientation or details about someone's sex life;
* or genetic or biometric data.

Bulk data

6. A defence Personal Information (PI) bulk data asset is defined as that containing:
a. More than 10k personal records; OR
b. More than 1k personal sensitive records; OR
c. Any identifiable protected population; AND
d. Defence is the data controller (either alone or jointly or in common with other persons) or the data processor.

7. A Defence Critical bulk data asset is a dataset that is not considered as personal bulk data and directly or indirectly supports, or enables, one or more of the following areas:
a. Defence strategic aims (for example, ongoing military operations, or the nuclear enterprise and the continuous at seas deterrent or future planning and the implementation of SDSR); OR
b. Would cause significant departmental reputational damage; OR
c. Compliance with legal and regulatory requirements; AND
d. Is processed in a dataset of more than 100,000 records.

You may wish to refer to the DAIS website, which gives more information about Bulk Data.

Annex B
Part 2's Pre-Screening Weighting Guide

This is a guide only. Please also refer to your own professional experience and any other advice you receive.

As a guide, if you score 4 or more points, then you are strongly advised to conduct a DPIA. As you will observe, two or more 'yes' answers will likely hit the threshold.

When considering all the information supplied at Part 1, you may still advise a DPIA is required, even if less than 4 points are scored.

Part 2B - Potential risk questions		**Weighting Guide**
Will this processing involve:		
1	Collecting personal data that is currently not held by the MOD?	1
2	Using personal data already held by the MOD, but for a new reason?	1
3	Processing personal data on a new asset / system / device? *(If yes, please ensure you **record this** on the information asset register - see guidance)*	1
4	Processing any security vetting data?	2
5	Processing ***any*** special category data?	2
6	Processing ***any*** personal information about children or vulnerable adults?	2
7	Processing personal data covering more than one TLB and / or Arms-Length Body?	1
8	Processing any biometric or genetic data?	3
9	Processing any personal data for national security / intelligence / law enforcement purposes?	2
10	Using personal information to evaluate or score the individuals concerned?	2
11	Giving parties outside MOD that previously did not have access to the data, access now? If yes, who?	3
12	Processing personal data outside the UK?	3

13	Processing personal data that might cause MOD serious reputational damage if it were to be unlawfully disclosed or accessed, lost, altered or destroyed?	3