

Data Protection Impact Assessment



Please send general queries about the DPIA process or form and / or return the form to DPO@bracknell-forest.gov.uk, copying in your IG Lead.

Title of DPIA	Example: Artificial Intelligence in Customer Calls
	Environmental monitoring of closed landfill sites
Brief summary of the project/ initiative	Example: We are looking to use artificial intelligence to determine the intent of the caller for some of our services.
	<p>The current contract for environmental monitoring is due to expire at the end of December 2022. As part of the tender process a DPIA assessment is required as an annex to the procurement plan which is signed off and agreed at Executive.</p> <p>The contract collects a small number of names, contact numbers and address details from residents that live in close proximity to London Road Landfill site as their properties are monitored for gas emissions. Residents sign a form to confirm their contact details can be passed onto an external contractor These details are stored by enitial (current contractor) and used as required for gas monitoring visits.</p>

Contact Details			
Author of this DPIA (Business owner)			
If the IG Lead is completing this document, the Business Owner should also be identified			
Name of Author	Damian James		
Job Title	Assistant Director: Contract Services		
Department/Team Name	Delivery – Contract Services		
Email	Damian.james@bracknell-forest.gov.uk	Tel No.	1325
Business Owner (if different from Author)			
Project Sponsor/Director/Information Asset Owner			
Name	Damian James		
Job Title	Assistant Director: Contract Services		
Date of submission	01/02/2022		

Purpose of a DPIA

The purpose of a DPIA is to assess the risks to people's personal data. By completing the steps in this DPIA, we identify, analyse and minimise the risk.

This DPIA is not a one-off exercise and recommendations should be added into project/service plans. This DPIA should be reviewed per the DPIA Tracker (please contact your [IG Lead](#) or the [DPO Mailbox](#) if you are unsure).

When completing the DPIA think about the best interests of the data subject(s), security and protection measures you would want putting in place to address risk if it were your data!

Checklist - Initial Assessment

If you answer no to everything below you can stop here, it is unlikely that a full DPIA is needed. You must still send this form to the DPO Mailbox DPO@bracknell-forest.gov.uk please copy in your [IG Lead](#) for awareness.

If you answer yes to any of the following you must complete the remainder of this document. You must then send it to the DPO Mailbox DPO@bracknell-forest.gov.uk please copy in your [IG Lead](#) for awareness:

- use systematic and extensive profiling or automated decision-making to make significant decisions about people;
- process special-category data or criminal-offence data on a large scale;
- systematically monitor a publicly accessible place on a large scale;
- use innovative technology in combination with any of the criteria in the European guidelines;
- use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
- carry out profiling on a large scale;
- process biometric or genetic data in combination with any of the criteria in the European guidelines;
- combine, compare or match data from multiple sources;
- process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;
- process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;
- process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;
- process personal data that could result in a risk of physical harm in the event of a security breach;
- if there is a change to the nature, scope, context or purposes of our existing processing.

Procurement and Legal Advice

Procurement engagement, support and approval		
Is there a procurement aspect to your project/ initiative?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Has a member of BFC procurement been involved in developing this proposal?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
If YES, name procurement professional:		
If there is a procurement aspect, you must ensure Procurement have had input into this DPIA.		

ICT engagement, support and approval		
Is there an IT aspect to your project/ initiative?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Has an BFC ICT Business partner been involved in developing this proposal?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
If YES, name the ICT Business Partner:		
If there is an ICT aspect, you must ensure ICT have had input into this DPIA.		

1. Project description

Provide a full description of the project, initiative or service
Please choose all of the below that apply to the project, initiative or service you are delivering
<ul style="list-style-type: none"> <input type="checkbox"/> The collection of new information about individuals <input type="checkbox"/> Compelling individuals to provide information about themselves <input type="checkbox"/> The disclosure of information about individuals to organisations or people who have not previously had routine access to the information <input type="checkbox"/> The use of existing information about individuals for a purpose it is not currently used for, or in a way it is not currently used <input type="checkbox"/> Contacting individuals in ways which they may find intrusive <input type="checkbox"/> Making changes to the way personal information is obtained, recorded, transmitted, deleted, or held <input type="checkbox"/> The use of profiling, automated decision-making, or special category data to make significant decisions about people (e.g. their access to a service, opportunity, or benefit) <input type="checkbox"/> The processing of special category data or criminal offence data on a large scale <input type="checkbox"/> Systematically monitoring a publicly accessible place on a large scale <input type="checkbox"/> The use of new technologies <input type="checkbox"/> Carrying out profiling on a large scale <input type="checkbox"/> Processing biometric or genetic data <input type="checkbox"/> Combining, comparing, or matching data from multiple sources <input type="checkbox"/> Processing personal data without providing a privacy notice directly to the individual <ul style="list-style-type: none"> <input type="checkbox"/> Processing personal data in a way which involves tracking individuals' online or offline location or behaviour <input type="checkbox"/> Processing children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them <input type="checkbox"/> Processing personal data which could result in a risk of physical harm in the event of a security breach
<p>What are the project's objectives/ scope/ benefits?</p> <p style="color: #666; font-size: small;">Click or tap here to enter text.</p>

Nature of personal information							
Forename	<input type="checkbox"/>	Surname	<input type="checkbox"/>	Postal address	<input type="checkbox"/>	Post code	<input type="checkbox"/>
Email address	<input type="checkbox"/>	Age	<input type="checkbox"/>	Date of Birth	<input type="checkbox"/>	Gender	<input type="checkbox"/>
Mobile Number	<input type="checkbox"/>	Telephone Number	<input type="checkbox"/>	NI Number	<input type="checkbox"/>	NHS number	<input type="checkbox"/>
Unique ID number (e.g. Mosaic ID)	<input type="checkbox"/>	Online identifier (IP address etc.)	<input type="checkbox"/>	Voice recording	<input type="checkbox"/>	Image (photo or video of person)	<input type="checkbox"/>
Personal financial details	<input type="checkbox"/>	No personal data held	<input type="checkbox"/>				
Other:							
Which of the following special category data will be used							
Criminal allegations convictions or offences	<input type="checkbox"/>	Data concerning health information	<input type="checkbox"/>	Data concerning sex life or orientation	<input type="checkbox"/>	Religious or philosophical beliefs	<input type="checkbox"/>
Political opinions	<input type="checkbox"/>	Racial or ethnic origin	<input type="checkbox"/>	Biometric data	<input type="checkbox"/>	Genetic data	<input type="checkbox"/>
Trade Union membership	<input type="checkbox"/>	No special category data	<input type="checkbox"/>				
Number of individuals with which personal data will be processed							
0 - 100	<input type="checkbox"/>						
100 - 1000	<input type="checkbox"/>						
1000 – 5000	<input type="checkbox"/>						
5000 +	<input type="checkbox"/>						
What geographical area does it cover?							
UK	<input type="checkbox"/>						
EU	<input type="checkbox"/>						
International	<input type="checkbox"/>						

2. Describe the processing

Describe the nature of the processing

How will you collect, use, store and delete the data?

Collect:

Click or tap here to enter text.

Use:

Click or tap here to enter text.

Store:

Click or tap here to enter text.

Delete:

Click or tap here to enter text.

What is the source of the data?

Click or tap here to enter text.

Will you be sharing data with anyone?

Yes	<input type="checkbox"/>
No	<input type="checkbox"/>

If yes, please list who you will be sharing the data with

Click or tap here to enter text.

Describe the scope of the processing

How often will you be collecting personal data?

Daily	<input type="checkbox"/>
Weekly	<input type="checkbox"/>
Monthly	<input type="checkbox"/>
Annually	<input type="checkbox"/>
Other	

How long will you keep it?

If this is different for different types of data, you can choose more than one and describe each in the text box below

0 – 1 year	<input type="checkbox"/>
1 – 5 years	<input type="checkbox"/>
5 – 10 years	<input type="checkbox"/>
10 – 20 years	<input type="checkbox"/>
Indefinitely	<input type="checkbox"/>
Other	<input type="checkbox"/>

Click or tap here to enter text.

Describe the context of the processing

What is the nature of your relationship with the individuals?

Click or tap here to enter text.

Is there another way to achieve the same outcome you are trying to reach?

Click or tap here to enter text.

How much control will individuals have?

Click or tap here to enter text.

Do the individuals include children or other vulnerable groups?

Click or tap here to enter text.

Are there prior concerns or security flaws around this type of processing?

Click or tap here to enter text.

Is the processing novel in any way?

Click or tap here to enter text.

What is the current state of technology in this area?

Click or tap here to enter text.

Are there any current issues of public concern that you should factor in?

Click or tap here to enter text.

Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Click or tap here to enter text.

What is the retention period for this information?

Click or tap here to enter text.

How will this information be deleted/ destroyed?

Click or tap here to enter text.

3. Consultation process

Consider how to consult with relevant stakeholders

Describe when and how you will seek individuals' views, or justify if it is not appropriate to do so.

Click or tap here to enter text.

Describe when and how you have consulted partner organisations, or explain why it is not appropriate to do so.

Click or tap here to enter text.

Who else have you involved within the Council?

Click or tap here to enter text.

Do you have a processor? Do you need to ask your processors to assist?

Click or tap here to enter text.

Do you plan to consult information security experts, or any other experts?

Click or tap here to enter text.

Do you have a relevant privacy notice that includes this processing? How will you actively provide this privacy information to individuals?

Click or tap here to enter text.

4. Compliance and Proportionality

To be completed with guidance from Legal Services if necessary

What is your lawful basis for processing?

- Public task: we need to process the data to perform a specific, necessary task that is in the public interest and is set out in law
- Consent: the data subject consents to the processing of their personal data
- Contract: we need to process the data to fulfil our contractual obligation with the individual
- Legal obligation: we need to process the data to comply with the law
- Vital interest of the data subject: we need to process the data to protect the individuals' life
- Legitimate interest (as a public body, this basis is very unlikely to apply and you must complete the [Legitimate Interest Assessment](#) before choosing this)

If you have chosen legal obligation or public task, identify the legislation / authority (e.g. Children Act (2004), Health and Social Care Act (2012) Crime and Disorder Act (1998))

Click or tap here to enter text.

Does the processing actually achieve your purpose?

Click or tap here to enter text.

How will you prevent function creep?

Click or tap here to enter text.

How will you ensure data quality and data minimisation?

Click or tap here to enter text.

What information will you give individuals (e.g. a relevant Privacy Notice)?

Click or tap here to enter text.

How will you help to support individuals' rights (e.g. inform them of their data rights)?

Click or tap here to enter text.

What measures are in place to ensure processors comply with relevant data protection requirements?

Click or tap here to enter text.

Do you make any international transfers? If, so what safeguards are in place?

Click or tap here to enter text.

5. Risk Review – Identify measures to reduce risk (to be completed by business owner with support from Audit and Risk Management if needed)

The following is the Council’s risk assessment matrix. It combines a risk rating from low to very high, derived from a combination of the likelihood of a risk occurring, coupled with the impact if it does. It, and the Likelihood and Impact scoring guides below should be used to assign pre and post mitigation risk scores in the risk log in the following section.

RISK MATRIX

LIKELIHOOD	5	Medium	High	High	High	High
	4	Medium	Medium	High	High	High
	3	Low	Medium	Medium	Medium	High
	2	Low	Low	Low	Medium	Medium
	1	Low	Low	Low	Low	Medium
		1	2	3	4	5
		IMPACT				

Likelihood:

- 5 Very High
- 4 High
- 3 Significant
- 2 Low
- 1 Almost Impossible

Impact:

- 5 Catastrophic 80%+
- 4 Critical 51% – 80%
- 3 Major 21% – 50%
- 2 Marginal 6% – 20%
- 1 Negligible 0% – 5%

The risk log below should detail privacy risks that the project/initiative may give rise to; mitigations with completion dates; pre and post-mitigation risk ratings and mitigation action owners (i.e. the name of the person who is responsible for carrying out the actions required to mitigate the risk(s). The Information Asset Owner / Project Sponsor etc. will be accountable for ensuring the mitigations are completed. Mitigating actions should be incorporated in project plans.

This information should be incorporated into the project plan/ proposal documentation

KEY: L = Likelihood of the risk occurring I = Impact of the risk occurring [see BFC risk matrix to apply scoring 1 to 5 in each case to drive a score]

#	Risk Description There is a risk that Giving rise to	Pre-Mitigation			Mitigating Action(s) and	Action Owner (i.e. who is responsible for the action)	Due Date	Status	Post-Mitigation		
		L	I	Risk					L	I	Risk
e.g. only	Mobile equipment (laptops) will be lost resulting in loss of / unauthorised access to personal data	4	5	H	Laptops to be encrypted by ICT prior to roll-out. Reporting system for lost equipment in place	Claire Smith	30/9/18	Live	2	4	M
e.g. only	Data will be accessed by people who are not authorised to view it resulting in increased privacy risks	5	3	H	Access controls to be set within CareCounts system and administered by X. Reports will be generated every X months and access will be checked by Y with action taken accordingly.	Robert Patel	31/12/18	Live	2	3	L
1											
2											
3											
4											
5											
6											
7											
8											
9											

8. Sign-Off, Advice and Approvals

Business Owner Sign-off

This DPIA is an accurate account of the project / initiative and Data Protection and Security measures that will be applied. Outstanding risk mitigations will be incorporated into project plan or service delivery.

Comments:

Click or tap here to enter text.

Name		Date	Click here to enter a date.
Signature			

DPO Sign-off

The DPO's advice is based on an assessment of the DPIA and whether proportionate and appropriate technical and organisational measures have been put in place to uphold an individuals' right to privacy.

Recommendation, comments and sign-off

Accept that no full DPIA is required

DPO comments/rationale as to why no full DPIA required:
Click or tap here to enter text.

Date of sign off:

Approve full DPIA as drafted

DPO comments/advice:
Click or tap here to enter text.

Date for review:
Date of sign off:

Approve full DPIA subject to conditions

Conditions and rationale:
Click or tap here to enter text.

Date for review:
Date of sign off:

Reject full DPIA as drafted

DPO comments/advice:
Click or tap here to enter text.

Date of next DPO review:

Refer full DPIA to ICO

Reason for referral to ICO:

Click or tap here to enter text.

Date of referral:

ICO response:

Click or tap here to enter text.

Actions taken and next steps:

Click or tap here to enter text.

DPO request for assurance from Legal Services

Legal advice sought?

Yes

No

Legal advice/ recommendations

Click or tap here to enter text.

Advised by

Date advice received

SIRO/Caldicott Guardian decision

Before signing the DPIA, the SIRO/Caldicott Guardian must ensure that they have considered advice of the DPO and are satisfied that the impact assessment is robust, has addressed all the relevant issues and that appropriate actions have been taken. Where the advice of the DPO has not been accepted, the rationale should be set out below.

Caldicott Guardian Decision, comments and sign-off

Have you considered and accepted the DPO's recommendation?

Yes

No

If no, please record rationale:

Click or tap here to enter text.

Approve DPIA as drafted

Caldicott Guardian comments/advice:

Click or tap here to enter text.

Approve DPIA subject to conditions

Conditions and rationale:

Click or tap here to enter text.

Date for review:

Date of sign off:

Reject DPIA as drafted

Caldicott Guardian comments/advice:
Click or tap here to enter text.

Refer to ICO

Reason for referral to ICO:
Click or tap here to enter text.

Date of referral:

ICO response:
Click or tap here to enter text.

Actions taken and next steps:
Click or tap here to enter text.

SIRO Decision, comments and sign-off

Have you considered and accepted the DPO's recommendation?

Yes

No

If no, please record rationale:
Click or tap here to enter text.

Approve DPIA as drafted

SIRO comments/advice:
Click or tap here to enter text.

Reject DPIA as drafted

SIRO comments/advice:
Click or tap here to enter text.

Approve DPIA subject to conditions

Conditions and rationale:
Click or tap here to enter text.

Date for review:
Date of sign off:

Refer to ICO

Reason for referral to ICO:

Click or tap here to enter text.

Date of referral:

ICO response:

Click or tap here to enter text.

Actions taken and next steps:

Click or tap here to enter text.

DPIA approval details logged on the DPIA tracker

Click here to enter a date.

Document	Title/Summary
Legal Including: Information Security Questionnaires; Privacy Notices, Consent Forms, Information Sharing Agreements, Data Processing Agreements, documentation of suitable safeguards for transfers of personal data to a third country or an international organisation	
	[Embed Doc]
	[Embed Doc]
Project Including: Business cases, PIDs, training documents, procedures	
Design & ICT Security Including: Spec, Security Assessments, Network Diagrams etc.	
	[Embed Doc]
	[Embed Doc]
Procurement Including: IG evaluation(s), Contract/Agreement	
	[Embed Doc]
	[Embed Doc]