DATA PROTECTION IMPACT ASSESSMENT (DPIA)

GUIDANCE

1. INTRODUCTION

1.1. Data Protection Impact Assessments (DPIA) are an integral part of the principle of privacy by design introduced by the General Data Protection Regulation 2016.

It is also a requirement under the Data Protection Act 2018 when processing information for a law enforcement reason, for example a process to carry out examination of large quantities of data to assist in the prosecution of health and safety breaches by the Council.

1.2. A DPIA is a process which minimises the privacy risks of new projects or work activities by considering how the proposed project or activities would impact on individuals involved to ensure that risks and potential issues are identified at the outset.

1.3. This policy and procedure is based on guidance produced by the Information Commissioner's Office, which can be accessed:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

2. WHEN IS A DPIA REQUIRED

2.1. The Council is obliged to carry out a DPIA when implementing new processes, system(s), changing an existing process or system(s), project or work that may impact on the privacy of individuals, or carrying out systematic processing of large quantities of personal data especially if special categories of personal data are being processed.

3. STAGES OF A DPIA

3.1. The initial screening stage:

3.1.1. To be completed by the project lead or responsible officer who will be delivering the proposed change. The screening questions are there to assess whether a DPIA should be carried out.

3.1.2. If the answers are no to the screening questions a DPIA is not required.

3.1.3. If any of the answers to the screening questions is yes then a DPIA is required.

3.1.4 Not all DPIA's must be sent to the ICO however we must consult the ICO if the DPIA identifies high risk processing and the Council cannot take measures to reduce the risk. The Council in these circumstances cannot start processing until we have consulted the ICO. It is therefore important to produce a comprehensive DPIA to prevent undue delays.

3.2. DPIA

3.2.1. The answers to the screening questions will indicate the depth of the DPIA required. If the answers to the screening questions are not known or more information is required it is best to re-visit once the information is available to decide at that point if a DPIA is required.

3.2.2. The project lead or responsible officer is required to fill out the DPIA and send to the Data Protection Officer who will offer guidance if needed.

3.2.3. There are three possible outcomes to the initial DPIA:

- The initial DPIA will be incomplete and will need to be further information.
- The initial DPIA is complete and no or low risk is identified that can be managed by the Council.
- The initial DPIA is complete and the Council cannot put in or guarantee adequate controls and must be reported to the ICO prior to any processing taking place. The implementation of the project **must be postponed at this point.**

3.3. Identifying risks

3.3.1. Identifying of risks involved with the processing of the data must be identified. The project lead or responsible officer must develop an action plan on how those risks will be mitigated and if they cannot be why they cannot be.

3.3.2. Identification of who is responsible for managing the risk must be included, if high risk this must be communicated to the DPO and s151 officer for inclusion on the Council's corporate risk register.

4. MEASURES TO REDUCE RISK

4.1. The aim of the DPIA is not to eliminate all risk regarding data privacy but to reduce to an acceptable level that protects the rights of the data subjects whilst enabling the Council to carry out its functions. If there is a high risk to the rights of data subjects but this risk is manageable then it does not mean the project cannot go ahead. It may mean that the decision if there are enough technological and organisational safeguards in place will be a decision of the ICO.

4.2. Examples of measures (this is not an exhaustive list but a guide only):

- Obtain the data subject's consent (only if they can give freely and withdraw their consent freely this is not usually a legitimate ground for processing for the Council as most activities carried out consent cannot be given freely as required by the GDPR and DPA 2018).
- Deciding not to collect or store particular data
- Only keeping the information as long as needed (guidance is in the Council's Records Retention Policy) and securely destroy either by shredding then placing in the confidential waste or arranging secure on site shredding obtaining a certificate of destruction a copy of which must be passed to the DPO.
- Ensure that the appropriate operational and technological security measures are in place – liaise with ICT.
- Restrict access to the processing to only those that need to.
- Prevent other systems from accessing – if appropriate.
- Keep data up to date have systems to be able to delete from systems
- Have ways to anonymise or pseudonymise the data ensuring that it cannot be reversed.
- Encryption of data
- Using only secure email
- Ensure training is given on how to use new systems

- Make sure systems are cyber secure to the Cyber Essential standards
- Ensure patches are always applied when required.
- Ensure data sharing agreements are in place clearly identify who is the controller and who is the processor or is it a controller to controller arrangement – incorporate into the contract
- Ensure those we contract with have the necessary organisational and technological systems in place only contract with those that do.
- Ensure that all procurement is compliant with the data principles in the GDPR and DPA 2018.

5. INTEGRATING DPIA OUTCOMES INTO THE PROJECT PLAN

5.1. The DPIA must be integrated into the project plan, the project lead must ensure compliance with the steps recommended in the DPIA and review at regular intervals.

5.2. As the project progresses if there are any risks that had not been identified the DPIA should be updated and an amended copy sent to the DPO. If the emerging risk has been assessed as being high and the Council is unable to mitigate it the project should be suspended and the DPO informed. The outcome may be that the ICO will need to be informed at this point to determine if the project can continue as is or what action needs to be taken to ensure that the risks are acceptable.

APPENDIX 1

Data Protection Impact Assessment

DPIA – Initial screening

Project Name	Spencetrs Croft
Brief outline of the project	Fire Safety and External Refurbishment
Project lead	D Coleman
Project dates (to – from)	TBA

1. Screening Questions:

These questions are designed to determine if a DPIA is necessary. If the answer to any of the first eight questions is yes a DPIA **may be required.**

Once completed please forward to the DPO for review who will offer guidance to the process.

Question	Yes	No	notes
1. Will the project involve the collection of new information/data about individuals?	☐	☑	
2. Will the project compel individuals to provide information/data about themselves?	☐	☑	
3. Will the information/data about individuals be disclosed to organisations or people who have not previously had routine access to the data?	☐	☑	
4. Are you using the information about individuals for a purpose it	☐	☑	

not currently used for, or in any way not currently used?			
5. Does the project/contract involve the use of new technology that might be privacy intrusive? Eg face recognition	☐	☑	
6. Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	☐	☑	
7. Is the information about individuals of the type that may cause privacy concerns? i.e. medical, criminal, biometric etc.	☐	☑	
8. Will the project require you to contact individuals in a way they would consider intrusive?	☐	☑	
9. Are you satisfied that the organisational and technological safeguards are in place?	☑	☐	
10. Are you satisfied that the data is not being processed in a country outside the EU or EAA?	☑	☐	

2. DPO Review

APPENDIX 2

Data Protection Impact Assessment (DPIA)

Project Name	
Brief outline of the project	
Project lead	
Project dates (to – from)	

Step 1: Identify the need for a DPIA

Identify the need for a DPIA: Explain broadly what the 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.

Step 2: Describe the processing

Describe the nature of 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 another way of describing data flows. What types of processing identified as likely high risk are involved?

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?

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)?

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?

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?

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?

Step 5: Identify and assess risks

Describe the 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

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**

Item	Name/Date	Notes
Measures approved by:		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
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted by or overruled by:		If overruled you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		

This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix 3

Data Protection Impact Assessment

(DPIA) Identifying compliance risks

Project Name	
Brief outline of the project	
Project lead	
Project dates (to – from)	

The following questions will help to identify where there is a risk the project will fail to comply with the Data Protection Principles set out in the General Data Protection Regulation and the Data Protection Act 2018

Data protection principle	Question	Answer
Processing data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.	Has the purpose of the project been identified?	
	How will individuals be told about the use of their data?	
	Does a privacy notice need amending or drafting?	
	Have the conditions for processing been identified?	
	If “consent” is required, how will this be documented? Collected, withdrawn or withheld?	
Personal data shall be collected for a specified, explicit and legitimate purposes	Does the project identify all the purposes for processing the personal data?	

	Have potential new purposes been identified as the scope of the project expands?	
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.	Is the information of good enough quality for the purposes it is to be used for?	
	Which data does not have to be used without compromising the project?	
Personal data shall be accurate and kept up to date	Does any new software or process enable the data to be amended if necessary?	
	If data is received from a third-party how will the accuracy be checked?	
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary	What retention period applies (note depending the purpose of the processing there may be more than one)?	
	Can the Council delete the information in line with the Retention Period?	
Personal data shall be processed in a manner that ensures appropriate security of the personal data	Will new or updated systems provide protection against security risks?	
	Will access be restricted?	
	What training will be given?	