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.