South Kesteven District Council

Procedure for undertaking a data protection impact assessment

December 2020

1 Introduction

1.1 Under previous legislation, the carrying out of a Data Privacy Impact Assessment (DPIA) was good practice. Completing a DPIA is now mandatory in certain circumstance in both the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). If you are introducing, changing, or assessing a process that handles personal data, you must complete a DPIA. This is a key element of the new focus on accountability and data protection by design, and a more risk-based approach to compliance.

1.2 A DPIA is a process to help identify and minimise the data protection risks of a particular project or activity when the processing of personal data is likely to result in 'high risk to individuals rights or freedoms'. A high risk might arise if the Council is intending to process data that:

- Involves the use of special category (sensitive), or highly personal data;
- Concerns vulnerable adults or children;
- Involves preventing people from using a service or exercising a right;
- Includes processing data on a large scale.

1.3 If you are in any doubt as to whether you need to complete a DPIA, you should consult with South Kesteven District Council's Data Protection Officer. Email: dpo@southkesteven.gov.uk

1.4 If you identify a high risk and you cannot mitigate that risk, you must consult with the DPO who will contact the Information Commissioner's Office (ICO) before starting the processing. The ICO will give written advice within 8 weeks, or 14 weeks in complex cases. In appropriate cases, the ICO has the power to issue a formal warning not to process the data, or to ban the processing altogether.

2 When should a DPIA be undertaken?

2.5 A DPIA is a process to systematically analyse the Council's processing and help SKDC to minimise data protection risks. It is intended to be an ongoing process; it should be monitored and reviewed as necessary. A DPIA must:

- Describe the processing and its purposes;
- Assess necessity and proportionality;
- Identify and assess risks to individuals; and
- Identify any measures to mitigate those risks and protect the data.

2.6 The GDPR states that the Council must carry out a DPIA if it plans to:

- Systematically monitor a public place on a large scale by for example, installing CCTV cameras;
- Process special category data or criminal offence data on a large scale;
- Use systematic and extensive profiling with significant effects;
- Use new technologies, process biometric data (e.g. fingerprints, facial recognition, retinal scans) and geometric data (an individual's gene sequence);
- Profile children or target services at them;
- Match data or combine data sets from different sources;
- Process personal data without providing a privacy notice directly to an individual;

- Process personal data that might endanger an individual's health or safety in the event of a security breach.

2.3 The GDPR also provides that the Council must, where appropriate, seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

The following checklist will assist you in terms of determining whether DPIA must be carried out.

		DPIA questions	**Yes/No**
1.	**Identity**	Will the project involve collecting information about individuals for the first time?	
2.	**Identity**	Will your project or activity compel individuals to provide information about themselves?	
3.	**Sharing information**	Will any information about individuals be disclosed to any other organisations?	
4.	**Data**	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
5.	**Data**	Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition or CCTV cameras?	
6.	**Data**	Will the project result in you making decisions or taking action against individuals in ways that could have a significant impact on them?	
7.	**Data**	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	
8.	**Data**	Will the project or activity require you to contact individuals in ways that they may find intrusive?	

If you have answered YES to ANY of the questions in the checklist, you will need to consult with the DPO.

3 What should a DPIA contain?

3.1 Section 64 of the DPA 2018 prescribes that a DPIA must contain as a minimum:

3.2 A systematic description of the proposed processing and its purpose;

3.3 An assessment of the risks to the rights and freedoms of data subjects;

3.4 The measures proposed to address those risks;

3.5 Safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Council's revised Data Protection Policies and Procedures.

The Data Protection Impact Assessment Template can be found on Monty or requested from the DPO and should be used when carrying out a DPIA.