CORPORATE AND COMMUNITY SERVICES

Data Protection Impact Assessment Guidance

DECEMBER 2019

North Kesteven
DISTRICT COUNCIL

Date of publication:	April 2018
Reviewed & updated:	December 2019
Next review:	December 2021

Alternative Formats

This document can be made available in large print, braille, audio tape, electronic formats such as CD, or in an alternative language. Our website is ReadSpeaker enabled. For a copy please contact the Corporate Information Team at the Council using the following options:

Phone: 01529 414155 (main switchboard)

Web: www.n-kesteven.gov.uk

Email: equality@n-kesteven.gov.uk

Corporate Information Manager
North Kesteven District Council
Kesteven Street
Sleaford
Lincolnshire
NG34 7EF

Contents

1. Introduction

The Information Commissioner's Office (ICO) defines a Data Protection Impact Assessment (DPIA) as: 'a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. They help identify privacy risks, foresee problems and bring forward solutions'.

a. What is a Data Protection Impact Assessment?

A DPIA is a process that assists organisations in identifying and minimising the privacy risks of new projects or policies. It will help to ensure that potential problems are identified at an early stage when addressing them will often be simpler and less costly. Conducting a DPIA should benefit the Council by producing better policies and systems, and improving the relationship with individuals.

b. Why should I carry out a DPIA?

Whilst not a legal requirement, it is often the most effective way to demonstrate to the ICO how personal data processing complies with the General Data Protection Regulations (GDPR) and Data Protection Act (DPA) 2018. A project or service which has been subject to a DPIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way. A DPIA should improve transparency and make it easier for individuals to understand how and why their information is being used.

c. When should I carry out a DPIA?

The core principles of a DPIA can be applied to any project or service that involves the use of personal data, or to any other activity that could have an impact on the privacy of individuals. Answering the screening questions in Stage 1 of the DPIA should help you identify whether there are privacy matters that need addressing.

d. Who should carry out a DPIA?

Responsibility for conducting a DPIA are best placed at Managers Forum level.

e. How do I carry out a DPIA?

The requirement for an assessment will be identified by answering the questions in Section 1 of the DPIA form. If a requirement has been identified, you should complete the remaining sections.

Within modern.gov, the DPIA template will automatically be at the end of your report, which you will need to send through the system for checking, further discussion and approval. The DPO will confirm whether the proposed measures address the privacy risks identified and could potentially make recommendations for additional measures needed. Once any required amendments have been made, the DPO will approve the DPIA via modern.gov allowing your report to progress through the system.

However, if you are unsure if a DPIA is required, please contact the DPO as early as possible on: dataprotection@n-kesteven.gov.uk

2. Specific Guidance to Assist with Completion of a DPIA

Section 1 – A DPIA is not applicable
Use this section to help determine if a DPIA is **not** required for your report. Select the reasons why an assessment is not required and use these to write a short summary to be included in the DPIA section of your report. Further sections can then be ignored.

Section 2 – A DPIA is necessary
Use this section to help determine the reasons why a DPIA is necessary for your report. If any of the listed statements are true then an assessment is necessary. In this case, please complete the remaining sections to provide further detail on the data protection impacts and risks associated with your report.

Section 3 – Data protection impacts
This section consists of a number of questions focusing on the data flows and processes involved with your project with the aim of assisting with the identification of possible sources of risk. Not all questions may be relevant to your project, for example you may not be sharing any information with third parties, so please answer 'No' or 'N/A' as appropriate.

a. Overview
   i. In your brief description of the policy/service/project aims and benefits, please include the purpose for which you are processing personal data. Explain why this processing is necessary for the purpose. Is there another way to achieve the purpose without processing personal data?
   ii. This may include consulting the data subjects (the individuals about whom personal data is held) on their views, discussions with contractors who may process the data or seeking advice from the DPO, ICT or others within the Council. If you are not consulting any stakeholders please justify your decision.
   iii. Information Asset Owners (IAOs) have the responsibility to ensure information is held and used appropriately, retained for the correct period of time and then correctly disposed of or transferred to the archives. The IAO should be the Manager or Team Leader responsible for the policy/service/project.

b. Collection
   i. Personal data is information that relates to an identified or identifiable individual, such as name or IP address.

      The GDPR and DPA define special category data as:
      - Personal data revealing racial or ethnic origin
      - Personal data revealing political opinions
      - Personal data revealing religious or philosophical beliefs
      - Personal data revealing trade union membership
      - Genetic data

- Biometric data (where used for identification purposes)
- Data concerning health
- Data concerning a person's sex life
- Data concerning a person's sexual orientation.

The GDPR rules for special category data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures.

The type of data and number of individuals are important in assessing the risks and potential impact of events, such as a data breach, for example, who are the data subjects – residents, tenants, colleagues?

ii. You must only collect the personal data that you actually need for your purpose. It must be sufficient but limited to what is necessary. You should also regularly review your data to ensure it is still required and delete it if it is no longer needed. Please detail how you will achieve this.

iii. Will you run a consultation or survey? Is personal data submitted as part of a process, for example, applications for a new parking permit scheme? Will you be transferring data from paper to an electronic document? How will you check input errors are not made?

iv. If you have a privacy notice informing data subjects of what you will do with their personal data please mention it here and ensure the DPO has created (or approved) before publishing it.

v. The personal data may be useful for a future purpose but, based on factors such as the legal basis for processing and terms of any privacy notice, this may not be possible. It is therefore useful to try and identity further purposes in advance.

vi. Lawful bases for processing are consent, contract, legal obligation, vital interests, public task and legitimate interest. At least one of these must apply in order to process personal data. The Information Commissioner's Office have produced an interactive tool for determining lawful basis which may be useful, please see https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool/ However, please see the DPO to discuss this further and review which lawful bases are applicable.

Please note that extra conditions must be met in order to process special category data, therefore please contact the DPO for guidance.

vii. Attach any consent documents to the assessment.

viii. Do you have any other legal bases for continuing to process the data? If not, if consent is withdrawn, how will you locate and destroy the personal data.

ix. If marketing is involved please briefly describe the opt-out process.

c. Storage and use

i. Will there be paper and/or electronic records containing the personal data? Will they be stored in a locked cupboard or on a shared drive, etc?
ii. Will it be up to individuals to keep you informed of any changes, such as change of address? Will you periodically recollect the data, for example by issuing a form to be reviewed or completed by the data subjects?
iii. Please note that data sharing with external organisations or people is covered in more detail in section (d). In these circumstances, please contact the DPO.
iv. Processing personal data away from the office will introduce risks, such as theft or loss of papers and electronic media. It is therefore important to note if this will occur and refer to the Council's Data Protection Policy and liaise with the DPO.

d. Sharing
   i. Third parties could include parish, district and county councils, leisure partners, contractors, etc.
   ii. This includes both physical and electronic transfers, for example using recorded delivery or encrypted email. Consider consulting ICT for guidance on electronic transfers.
   iii. Transfer of personal data outside the EEA is restricted as individuals risk losing the protection provided by the GDPR. Can you achieve your aims without transferring any personal data? Is your transfer covered by an EU Commission 'adequacy decision', 'appropriate safeguards' or an 'exception'?
   iv. Please provide the contractor name, location and the data they are processing and the reason for this.
   v. Please consider attaching a copy of the agreement with the contractor. How will they protect the data during processing, including storage and destruction? For further information, please contact the DPO.

e. Destruction
   i. The retention period, or how long the records will be kept, depends on the type of data and its purpose, as there may be legal requirements or best practice guidelines to abide by. For guidance, please consult the Record of Processing Activity and the DPO. In addition, it would be a good opportunity to note where the records are to be located.
   ii. How will you know/be reminded when to delete the data? How will you ensure that all copies, including all paper and electronic versions, are deleted at that time?

f. Other
   i. Please include any further information that is relevant to the assessment.

Section 4 – Risk Eeduction/Mitigation
This section consists of a table to identify and help reduce risks associated with your data processing.

It may be useful to review the data process, from collection to destruction, and the information provided in Section 3 in order to help identify the risks.

Completing the table:

a. Identify the risk giving detail on the source and the potential impact. Risks could include loss of confidentiality, identity theft, discrimination, financial loss, regulatory action, damage to reputation or loss of public trust.
b. Assess the likelihood of harm, rating it remote, possible or probable.
c. Assess the severity of harm, rating it minimal, significant or severe. For example, a data breach involving personal data such as names and email addresses could have less impact than a breach of special category data such as safeguarding or health information.
d. Using the grid below assign an overall risk based on the likelihood and severity of harm.

Table 1. Risk based on severity of impact and likelihood of harm

Severity of impact	Severe harm	Low risk	High risk	High risk
	Significant harm	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Possible	Probable
		Likelihood of harm		

e. If the risk is medium or high, please include options to reduce or eliminate the risk. This could include choosing not to collect certain types of data, introducing additional security measures, an improved privacy notice or data-sharing agreements. Is there a prohibitive cost associated with this measure?
f. Based on the options to reduce risk, please assess the residual risk as low, medium or high. However, it may not be possible to eliminate every risk. Therefore, some risk may be considered acceptable due to the benefits of processing the data and difficulties in mitigation.

An example ‘Data protection risks and risk reduction’ table is shown on page 10.

Section 5 – Monitoring and outcome

i. Will you check the DPIA periodically or at specific points within your project in order to manage risks? It will also be necessary to revisit or repeat the DPIA if there are changes to the nature, scope, context or purposes of your processing.

ii. This section should be completed by the DPO, which will be reviewed and approved as necessary. If changes have been made as a result of the review, these also need to be recorded.

Section 6 – Review and update

This section is not to be used on the initial completion of the impact assessment. This section should be completed if the review date is reached or based on a trigger event, such as changes to the processing of personal data associated with the project.

i. Provide a summary of the changes to the project and potential data protection impacts. How will changes in risk be managed?

ii. This section should be completed by the DPO.

This section may be duplicated to allow further reviews and updates.

If major changes are required consider completing a new DPIA form.

If you have any queries regarding the DPIA, please contact the DPO on: dataprotection@n-kesteven.gov.uk

3. Guidance Review

This guidance will be formally reviewed every two years to ensure it continues to be relevant and current. In some circumstances it may be necessary to review this guidance more frequently in response to specific events.

Table 2. An example of how to complete Section 4 of the DPIA

Section 4 - EXAMPLE **Data protection risks and risk reduction**					
Risk	Likelihood of harm	Severity of harm	Overall risk	Options to reduce or eliminate risk (if medium or high)	Residual risk
Data breach caused by loss of 200 paper surveys containing tenants' personal (not special category) data. Could cause distress to the individuals whose data is breached. Reputational damage to the council/negative publicity.	Possible	Significant	Medium	Retain completed surveys in a locked room when not in use. Do not allow paper surveys to be taken out of the office for processing/inputting.	Low
Data input errors in electronic records of customer calls relating to missed bins. Errors are likely to be low as names and addresses are checked against existing customer records. Impact – refuse collectors incorrectly informed of address, bin not collected, poor customer service.	Minimal	Remote	Low	N/A	N/A
Loss of control over use of personal data for over 1,000 identifiable individuals that has been shared with external processor. Distress to individuals, reputation damage, regulatory action against the council.	Possible	Severe	High	Ensure there is a contract in place to provide assurances on the data processing (including use, storage and destruction). Periodic GDPR compliance checks of the processor.	Low

North Kesteven
DISTRICT COUNCIL

District Council Offices, Kesteven Street, Sleaford, Lincolnshire NG34 7EF
Telephone Number: (01529) 414155
180912-JA2