

Data Protection Impact Assessment – Sancreed Parish Council

Background

Data Protection Impact Assessments are needed for all projects that involve processing personal data and any activities that affect the processing of personal data and impact the privacy of individuals.

To assess risks, the Council should carry out a Data Protection Impact Assessment (DPIA) for higher risk or changing activities. An example is included with the draft data protection policies to be considered at the meeting.

Advice from NALC is that for most day-to-day activities a short review is enough to show that the council has considered privacy and security, with the following prompts given as the basis for a light-touch risk review:

- What could go wrong?
- Who might be affected?
- How serious would it be?
- What can we do to reduce the risk?

Assessment process

This procedure sets out when and how to conduct a DPIA on activities, projects and processes. All staff and Councillors of the parish council are required to carry out a DPIA on new activities. The DPI should be carried out before starting any new activity.

1. Screening questions to identify whether a full DPIA is needed
2. If needed, DPIA process:
 - a. Describe the flow of information including details of the personal data to be collected, the basis for its lawful processing and any other information.
 - b. Identify the privacy and related risks, that will have an impact on individuals. i.e. nature of personal data being process, volume of data, manner in which it will be processed. Risks to be assigned a risk rating based on likelihood of occurrence and potential impact.
 - c. Identify and select privacy solutions. These will depend on the risk level and the potential mitigations available.
 - d. Approve the DPIA. Create a record to summarise the process and record decisions taken to eliminate, reduce, mitigate or accept the identified risks.
 - e. Integrate the DPIA outcomes into the project plan.
- 3.

Definitions

Personal Data: Any information relating to an identified or identifiable person (data subject). An identifiable person is someone who can be identified directly or indirectly, e.g. by an identifier such as name, address, online identifier, etc

Special Category Data: Data which requires extra care and precaution to be taken in processing and includes:

- Ethnicity
- Political views
- Religion
- Trade union membership
- Health / sexuality information
- Genetic or biometric data

Stage 1 – Screening questions

- 1) Describe the project/process, including aims and intended benefits
- 2) Is there a need to collect new information about individuals?
- 3) Will the information about individuals be disclosed to third parties who have not previously had access to the information?
- 4) Is the information about individuals of a kind likely to raise privacy concerns or expectations?
e.g. disability, vulnerability
- 5) Will the project result in decisions to act towards individuals in ways which could have a significant impact on them?

If the answer to the questions above is 'yes', then proceed to stage 2.

Stage 2: Full DPIA Review

Name of Project/Process:

*Other Organisations involved?

Section 1: General Information	Organisation Name	*
	Organisation Address	*
	Name and contact details (email/phone) of the person submitting the response	*
	Organisation Overview	*

Section 2: Data being Processed	Yes/No	Data Type	Yes/No	Data Type
Please indicate if any or all of this Personally Identifiable		Name, Address, DOB, Phone, Email		Location data
		Financial information		Disabilities
		Medical/Health information		Biometric or genetic information
		Information about behaviour		Profiling

Information (PII) is or will be processed		Criminal offences/convictions		Other (please specify)
		Religious Beliefs, Trades Union Membership or Political Opinions		Other identifiers e.g. username, twitter name etc.
		Photographs		

Section 2.1: Lawful Bases for Processing Please select which lawful bases for processing apply to the personal data identified as being processed in section 2.	Yes/No	Lawful Bases	Additional Information
		Processing is necessary for the performance of a contract with the data subject or to take steps to enter a contract. e.g. Employment Agreement	
		Processing is necessary for compliance with a legal obligation e.g. Safeguarding Laws	
		Processing is necessary to protect the vital interests of a data subject or another person	
		Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	
		Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject (please specify what the legitimate interests are in Additional Information)	
		Consent of the data subject	
		Other (please specify in Additional Information)	

Section 3: Data Flow Demonstrate how data is accessed, moved and saved.	<i>Where does data go?</i> Please outline how information moves from and to each of the devices and processes <i>Clarify how you encrypt data and when you do so.</i> <i>Where is the data to be stored/held?</i>
---	---

	<i>Where are devices that can access the data physically located</i> <i>How will it be stored?</i> <i>Will the data be available on the 'cloud'?</i> <i>How long will it be kept?</i> <i>How will it be deleted after use?</i>
--	---

Section 4: Data Subject Rights Please clarify how you can offer Data Subjects the following rights	Right to access	
	Right to have data rectified or erased	
	Right to restrict processing	
	Right to object to processing, automated decision making and profiling	
	Right to object to processing for the purposes of direct marketing	
	Right of data portability	*only applies if data held electronically
	Right to object to processing for scientific, historical or statistical purposes	

Classification: Confidential When Complete

DPIA Report

To include:

- Summary of project/process
- Privacy analysis – information collection and obtaining, use, disclosure and retention of information
- Privacy risk assessment outcomes
- Steps to be taken to ensure compliance with privacy and data protection legislation
- Conclusion