**Hinderclay Parish Council**

**Data Protection Impact Assessment Procedure**

## What is a Data Protection Impact Assessment (DPIA) and when is it needed?

A Data Protection Impact Assessment is a type of audit used to help assess privacy risks. A council might carry out a DPIA if it was going to outsource its payroll function for the first time or if it was installing CCTV which included cameras pointed at public areas.

A DPIA assesses the impact of any proposed processing operation, for example the use of new technology, on the protection of personal data. A DPIA should be carried out before the processing of the personal data starts and then updated throughout the lifetime of any project.

The content of a DPIA usually includes:
(a) A description of the processing activities and their purpose;
(b) An assessment of the need for and the proportionality of the processing; and
(c) The risks arising and measures adopted to try and prevent any risks, in particular any safeguarding or security measures to protect data and comply with the GDPR.

The DPIA checklist below can be used to help determine whether a DPIA is needed. The Article 29 Working Party, which is an independent agency that advises the European Union on data protection law, recently published guidance on when a DPIA is required. Their guidance is reflected in the DPIA Checklist.

## DPIA Assessment Checklist

Under the GDPR, data protection impact assessments (DPIAs) are mandatory where the processing poses a high risk to the rights and freedoms of individuals. While they can also be carried out in other situations, councils need to be able to evaluate when a DPIA is required. This checklist helps you make that assessment and provides a springboard for some of the issues you will need to consider in more detail if you do need to carry out a DPIA.

### 1. Do you need to carry out a DPIA?

(a) What is the objective/intended outcome of the project?
(b) Is it a significant piece of work affecting how services/operations are currently provided?
(c) Who is the audience or who will be affected by the project?
(d) Will the project involve the collection of new personal data about people? *(e.g. new identifiers or behavioural information relating to individuals?)*
(e) Will the project involve combining anonymised data sources in a way that may give rise to a risk that individuals could be identified?
(f) Will the project involve combining datasets originating from different processing operations or data controllers in a way which would exceed the reasonable expectations of the individuals?
(g) Is data being processed on a large scale?
(h) Will the project compel individuals to provide personal data about themselves?

(i) Will personal data about individuals be disclosed to organisations or people who have not previously had routine access to the personal data?
(j) Will personal data be transferred outside the EEA?
(k) Is personal data about individuals to be used for a purpose it is not currently used for, or in a way it is not currently used?
(l) Will personal data about children under 13 or other vulnerable persons be collected or otherwise processed?
(m) Will new technology be used which might be seen as privacy intrusive? (e.g. tracking, surveillance, observation or monitoring software, capture of image, video or audio or location)
(n) Is monitoring or tracking or profiling of individuals taking place?
(o) Is data being used for automated decision making with legal or similar significant effect?
(p) Is data being used for evaluation or scoring? (e.g. performance at work, economic situation, health, interests or behaviour)
(q) Is sensitive data being collected including:
    (i) Race
    (ii) Ethnic origin
    (iii) Political opinions
    (iv) Religious or philosophical beliefs
    (v) Trade union membership
    (vi) Genetic data
    (vii) Biometric data (e.g. facial recognition, finger print data)
    (viii) Health data
    (ix) Data about sex life or sexual orientation?
(r) Will the processing itself prevent data subjects from exercising a right or using a service or contract?
(s) Is the personal data about individuals of a kind likely to raise privacy concerns or is it personal data people would consider to be particularly private or confidential?
(t) Will the project require contact to be made with individuals in ways they may find intrusive?

## 2. Other issues to consider when carrying out a DPIA

(a) In addition to considering the above issues in greater detail, when conducting a DPIA, the following issues will need to be considered:
    (i) The lawful grounds for processing and the capture of consent where appropriate
    (ii) The purposes the data will be used for, how this will be communicated to the data subjects and the lawful grounds for processing
    (iii) Who the data will be disclosed to
    (iv) Where the data will be hosted and its geographical journey (including how data subjects will be kept informed about this)
    (v) The internal process for risk assessment
    (vi) Who needs to be consulted (DPO, data subjects, the Information Commissioners Office ("ICO"))

(vii) Data minimisation (including whether data can be anonymised)
(viii) How accuracy of data will be maintained
(ix) How long the data will be retained and what the processes are for deletion of data
(x) Data storage measures
(xi) Data security measures including what is appropriate relative to risk and whether measures such as encryption or pseudonymisation can be used to reduce risk
(xii) Opportunities for data subject to exercise their rights
(xiii) What staff or, as appropriate, councillor training is being undertaken to help minimise risk
(xiv) The technical and organisational measures used to reduce risk (including allowing different levels of access to data and red flagging unusual behaviour or incidents)

The General Data Protection Regulation (GDPR) requires that councils carry out a DPIA when processing is likely to result in a high risk to the rights and freedoms of data subjects. For a council, examples might include using CCTV to monitor public areas.

If two or more of the following apply, it is likely that you will be required to carry out a DPIA. This does not apply to existing systems but would apply if you introduced a new system:

1. Profiling is in use. Example: you monitor website clicks or behaviour and record people's interests. ☐
2. Automated-decision making. Example: when processing leads to the potential exclusion of individuals. ☐
3. CCTV surveillance of public areas. Processing used to observe, monitor or control data subjects. ☐
4. Sensitive personal data as well as personal data relating to criminal convictions or offences. ☐
5. Large scale data processing. There is no definition of "large scale". However consider: the number of data subjects concerned, the volume of data and/or the range of different data items being processed. ☐
6. Linked databases - in other words, data aggregation. Example: two datasets merged together, that could "exceed the reasonable expectations of the user". E.g. you merge your mailing list with another council, club or association. ☐
7. Data concerning vulnerable data subjects, especially when power imbalances arise, e.g. staff-employer, where consent may be vague, data of children, mentally ill, asylum seekers, elderly, patients. ☐
8. "New technologies are in use". E.g. use of social media, etc. ☐
9. Data transfers outside of the EEA. ☐
10. "Unavoidable and unexpected processing". For example, processing performed on a public area that people passing by cannot avoid. Example: Wi-Fi tracking. ☐

**Data Protection Impact Assessment Form**

**Submitting controller details**

| | |
|---|---|
| Name of controller | |
| Subject/title of DPO | |
| Name of controller contact /DPO (delete as appropriate) | |

## 1. Step 1: Identify the need for a DPIA

| Explain broadly what 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. |
|---|
| |

## 2. Step 2: Describe the processing

| **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? 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? |
| --- |
| |

## 3. 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 the Council? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts? |
| --- |
| |

## 4. 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? |
| --- |
| |

## 5. Step 5: Identify and assess risks

| **Describe 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** |
|---|---|---|---|
| | Remote, possible or probable | Minimal, significant or severe | Low, medium or high |

## 6. Step 6: Identify measures to reduce 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** |
| | | Eliminated<br>reduced<br>accepted | Low<br>medium<br>high | Yes/no |

## 7. Step 7: Sign off and record outcomes

| Item | Name/position/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 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 kept under review by: | | The DPO should also review ongoing compliance with DPIA |