Lower Hardres & Nackington Parish Council
GDPR Implementation & Compliance
Data Protection Impact Assessment (DPIA) Policy Document

Compiled – Mike Taylor – August 2018

Definition of "Data Protection Impact Assessment" (DPIA)

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.

DPIA Need Assessment Criteria

Under the GDPR, DPIAs are mandatory where the processing poses a high risk to the rights and freedoms of individuals. A DPIA ***may*** be necessary if two or more of the following apply. This does not apply to existing systems but would apply to 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, which 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. ☐

DPIA preparation Checklist.

The following summarises a checklist to be considered when preparation of a DPIA is deemed necessary.

(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?

Other issues to consider in carrying out a DPIA

(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)