The role of Data Protection Officers

1. What does a Data Protection Officer do?

(a) The GDPR sets out in detail the minimum responsibilities of the Data Protection Officer ("DPO") role. GDPR specifies that DPOs "should assist the controller or the processor to monitor internal compliance with this Regulation".

(b) A DPO's duties include:

(i) informing and advising the council and its staff of their obligations in the GDPR and other data protection laws;

(ii) monitoring compliance of the council, both its practices and policies, with the GDPR and other data protection laws;

(iii) raising awareness of data protection law; providing relevant training to staff and councillors;

(iv) carrying out data protection-related audits;

(v) providing advice to the council, where requested, in relation to the carrying out of data protection impact assessments ('DPIAs') and the council's wider obligations with regard to DPIAs; and

(vi) acting as a contact point for the Information Commissioner's Office.

(c) As part of these duties to monitor compliance, DPOs may, in particular:

(i) collect information to identify processing activities;

(ii) analyse and check the compliance of processing activities; and

(iii) inform, advise and issue recommendations to the controller or the processor

(d) Monitoring of compliance does not mean that it is the DPO is personally responsible where there is an instance of non-compliance. The GDPR makes it clear that it is the controller, not the DPO, who is required to 'implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.'

(e) The appointed DPO must at all times have regard to 'the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing.' This is an overarching obligation which means that the role of the DPO will vary in proportion to the risks to the rights of individuals affected by the council's processing of personal data.

(f) The DPO should 'cooperate with the supervisory authority' (in the UK, this is the Information Commissioners Office ("ICO") and 'act as a contact point for the supervisory authority on issues relating to processing, and to consult, where appropriate, with regard to any other matter'.

(g) It is the controller or the processor, not the DPO, who is required to 'maintain a record of processing operations under its responsibility' or 'maintain a record of all categories of processing activities carried out on behalf of a controller'.

2. DPOs and DPIAs

(a) A data controller (and not the DPO) is required to carry out a data protection impact assessment ('DPIA') under the GDPR in certain circumstances.

(b) The controller must 'seek advice' from the DPO when carrying out a DPIA. DPOs have the duty to 'provide advice where requested as regards the DPIA and monitor its performance'.

(c) It is recommended that controllers should seek the advice of the DPO on the following issues:

(i) Whether or not to carry out a DPIA;

(ii) What methodology to follow when carrying out a DPIA;

(iii) Whether to carry out the DPIA in-house or whether to outsource what it safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects; and

(iv) Whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR.

(d) If the controller disagrees with the advice provided by the DPO, the DPIA documentation should specifically justify in writing why the advice has not been taken into account.

3. Data controllers and processors should ensure that:

(a) The DPO is invited to participate regularly in meetings of senior and middle management. For councils, this would include meetings of full council and relevant committee meetings.

(b) The DPO's name and contact details are provided to ICO;

(c) The DPO should be available to advise/ support councillors and relevant staff on data protection issues;

(d) The DPO is present when decisions with data protection implications are taken;

(e) All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice;

(f) The opinion of the DPO must always be given due weight. In case of disagreement it is good practice to document the reasons for not following the DPO's advice;

(g) The DPO should be promptly consulted once a data breach or another incident has occurred. This is good practice since the DPO will often have been involved in implementing data protection polices such as breach reporting and it will be important for the DPO to assess whether the policies work operationally.

4. Role Checklist

- ☐ Raising data protection awareness within the council, and advising on GDPR compliance;
- ☐ Ensuring the implementation of the appropriate documentation to demonstrate GDPR compliance;
- ☐ Monitoring the implementation and compliance with policies, procedures and GDPR in general;
- ☐ Involvement in council's handling of data breaches, including assisting and advising the council with its notification to the ICO and data subjects where necessary (but it is the council which has the obligation to notify in certain circumstances not the DPO);
- ☐ Liaising with the ICO, the relevant councillors and staff and with the data subjects;
- ☐ Monitoring Data Protection Impact Assessments;
- ☐ Cooperating with and acting as the contact point for the ICO on issues relating to processing'