
Subject: THE GENERAL DATA PROTECTION REGULATION (GDPR) – DESIGNATION OF A DATA PROTECTION OFFICER (DPO)

Meeting and Date: COUNCIL – 7 MARCH 2018

Report of: David Randall, Director of Governance (Monitoring Officer)

Classification: UNRESTRICTED

Purpose of the report: To designate a data protection officer for the Council pursuant to the requirements of the GDPR

Recommendation:

- (1) That Harvey Rudd, the Solicitor to the Council be designated as the Council's data protection officer in accordance with Article 37 of the General Data Protection Regulation with effect from 25 May 2018.
- (2) That the Director of Governance (Monitoring Officer) be requested to make any necessary changes to the constitution consequent on (1) as part of his function of keeping the Constitution under review.

1. Introduction and Background

- 1.1 The General Data Protection Regulation (GDPR) will come into force on 25 May 2018. The GDPR replaces existing national laws relating to data protection and also the existing regulations based on the 1995 EU Data Protection Directive. As a regulation, the GDPR will have direct effect through the EU without requiring transposition into national legislation by member states.
- 1.2 As a public authority the Council is required by Article 37 of the GDPR to designate a data protection officer (DPO)

2. Tasks the DPO, Employer Responsibilities and Position of the DPO Within the Council.

- 2.1 The minimum tasks of the DPO are set out in Article 39 GDPR. These tasks are helpfully summarised in guidance issues in the following terms:-
 - To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
 - To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
 - To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).
- 2.2 The GDPR does not specify any particular qualifications that DPO must hold but does require that they should have professional experience and knowledge of data protection law and practice and the ability to fulfil the tasks required by Article 39.
- 2.3 The GDPR requires that the Council shall:

- Ensure that the DPO report to the highest level of management of the organisation,
- Ensure that the DPO is independent (in that he shall not receive any instructions regarding the exercise of his tasks nor be dismissed nor penalised for performing those tasks)
- Support the DPO by in performing his tasks and provided with adequate resources and training to meet his GDPR tasks.
- Ensure that the DPO does not undertake other tasks and duties which result in a conflict of interests.
- To publish the contact details of the DPO and to communicate those details to the relevant supervisory authorities (the Information Commissioner)

2.4 The so called Article 29 Working party¹ has issued further guidance with regard to the position of the DPO and the requirement for independence and absence of conflict of interest:- it has said:-

The absence of conflict of interests is closely linked to the requirement to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests. This entails in particular that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.

2.5 More particularly the working party has advised that there are certain positions which in an organisation will not be compatible with the DPO role:

As a rule of thumb, conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues.

2.6 The effect of the requirements for professional experience and knowledge of data protection law and practice, seniority, independence, and the absence of a conflict of interest combine to severely constrain the available choice of an existing employee of the Council to fulfil this role. Either the responsibilities of existing employees are not compatible with the role or their skills and knowledge of data protection law and practice is not at the level required for the DPO role.

2.7 Having reviewed the seniority, responsibilities and skills sets of existing employees it is considered that the present Solicitor to the Council should be designated as the DPO.

¹ The Working Party On The Protection Of Individuals With Regard To The Processing Of Personal Data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995

- 2.8 The Solicitor to the Council does not hold a specialist qualification in data protection law and practice however he has worked as a qualified solicitor in a local authority environment for in excess of 30 years during which he has gained extensive experience of data protection issues. More particularly he has knowledge of the business sector and of the organisation. He also has a good understanding of the processing operations carried out, as well as the information systems, and data security and data protection needs of the Council.
- 2.9 In terms of the independence requirement, the Solicitor to the Council holds a current practicing certificate, is fully cognisant of the need for professional independence in that capacity and is ultimately subject to regulation by the Solicitors Regulation Authority. He does not determine the purposes and means of data processing and the Constitution of the Council already makes provision for his access to senior management and members.

3. Identification of Options

- 3.1 Option 1 – To designate the Solicitor to the Council as a the DPO
- 3.2 Option 2 – To identify another employee within the organisation to designate as DPO
- 3.3 Option 3 – To create a new role of DPO and either recruit to it externally or appoint a consultant to the role.

4. Evaluation of Options

- 4.1 Option 1 is the preferred option. The Solicitor to the Council is suitable for designation to the role. His appointment would fulfil the legal obligations of the Council. This option does not give rise to a significant resource requirement. The Director of Governance (Monitoring Officer) will consider the extent to which it is necessary or desirable to make any changes to the Constitution arising from the designation of a DPO and will make recommendations as part of function of keeping the Constitution under review.
- 4.2 Option 2 is not a preferred option. The Council's choice of DPO from within those currently employed by the Council is constrained by the factors mentioned in paragraph 2.6.
- 4.3 Option 3. is not recommended. The creation of a new post of DPO and the recruitment of an individual to it (either as a direct employee or a consultant) would fulfil the Council's legal obligation. However it is considered that this goes beyond what is necessary and would have resource requirement extending beyond current budgets

5. Resource Implications

Provision for GDPR compliance is already included within the Council's existing budgets and proposed estimates. There is potentially a small ongoing training budget implication arising from the need to designate a DPO. If this proposal is approved that cost would be met from the existing corporate training budgets. It is not proposed that the salary of the Solicitor to the Council will be enhanced by his designation as DPO

6. Annex

Relevant extract from the GDPR

7. **Background Papers**

The GDPR

Article 29 Working Party Guidelines on Data Protection Officers ('DPOs')

Contact Officers: David Randall, Director of Governance and Monitoring Officer,
ext. 2141

Louise May, Head of Legal Services. 2328

Appendix 1

Relevant Extract from the GDPR

Data protection officer

Article 37

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:
 - (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
 - (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
 - (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.
2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment
3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.
4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.
5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.
6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.
7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 38

Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data
2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.
3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.
5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.
6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39

Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:
 - (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
 - (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
 - (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
 - (d) to cooperate with the supervisory authority;
 - (e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.
2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.