AUDIT COMMITTEE – 30TH JANUARY 2018

SUBJECT: **STATUTORY DATA PROTECTION OFFICER ROLE**

REPORT BY: **ACTING DIRECTOR OF CORPORATE SERVICES & SECTION 151 OFFICER**

---

1. PURPOSE OF REPORT

1.1 To ensure that Members are aware of the requirement to create a new statutory role of Data Protection Officer as prescribed by the forthcoming EU General Data Protection Regulation (GDPR) and seek the views of Members prior to presentation of the report to Cabinet.

2. SUMMARY

2.1 The GDPR will come into force on 25th May 2018 introducing a new requirement for organisations to have a statutory role of Data Protection Officer (DPO). This report proposes how this function could be delivered in CCBC.

3. LINKS TO STRATEGY

3.1 Data protection and information governance is an important element in delivering council priorities and ensuring contribution to the well-being goals set out in the Well-being of Future Generations (Wales) Act 2015 (WBFGA):

- A prosperous Wales
- A resilient Wales
- A healthier Wales
- A more equal Wales
- A Wales of cohesive communities
- A Wales of vibrant culture and thriving Welsh Language
- A globally responsible Wales

4. THE REPORT

4.1 The GDPR will come into force on 25th May 2018, enhancing existing protections for personal data, introducing new requirements and increasing the maximum monetary penalty for data breaches from £500,000 to €20 million or 4% of global annual turnover.

4.2 One of the new requirements is the need to introduce a new statutory role of Data Protection Officer (DPO) for the Council. Currently the Data Controller responsible for data protection compliance is the Council as a corporate body and not a specific employee within the Council. However, responsibility for data protection has been delegated to the Corporate Information Governance Unit (CIGU) which is overseen by the Senior Information Risk Owner (SIRO) and the new statutory role will build on this existing sound foundation.

4.3 The GDPR offers advice regarding the responsibilities and options for organisations relating to the DPO role. The salient points have been extracted and provided as Appendix 1 for ease of reference.

4.4 Appendix 2 describes the current allocation of data protection duties within the Council outlining the broader information management role of the Corporate Information Governance Unit (CIGU) including the Corporate Information Governance Manager, the SIRO, the close relationships with Legal Services at Exemption Panel and all Service Areas via their Information Governance Stewards. The CIGU team members have qualifications and experience to satisfy the GDPR requirement for "professional experience and knowledge of data protection law that is proportionate to the level of protection that the personal data processed by the Council requires" as recommended by the Information Commissioner's Office (ICO) Guide to GDPR.

4.5 To assure the Council as Data Controller that information is managed consistently and risks are minimised across every Council service, the SIRO and information governance expertise provision are currently a corporate function. As this is the case, it would seem appropriate that the DPO is located within the corporate function also..

4.6 Having considered the GDPR guidance available, ICO advisory publications and current working practices and structure in place in CCBC, the most appropriate approach would be to allocate the DPO role to the Authority's Corporate Information Governance Manager (CIGM).

4.7 It is proposed to maintain a direct reporting line between the DPO and the more senior SIRO role as this keeps GDPR compliance consistent with the UK government approach to broader information risk.

5. WELL-BEING OF FUTURE GENERATIONS

5.1 This report contributes to the Well-being Goals as set out in Links to Strategy above. It is consistent with the five ways of working as defined within the sustainable development principle in the Act as detailed below:

5.1.1 Long Term – Effective and appropriate information governance, data protection and insight sharing is critical to future service provision.

5.1.2 Prevention - Effective and appropriate information governance, data protection and insight sharing will enhance service areas' capability to predict future service demand, identify trends and revise service plans or intervene to prevent a problem occurring or worsening.

5.1.3 Integration – Safe and appropriate sharing of information contributes to the Well-being Goals, the Council's own Well-being Objectives as well as those of other organisations.

5.1.4 Collaboration – Safe and appropriate sharing of information is a key element of collaboration projects.

5.1.5 Involvement – Although this report relates to a statutory requirement, an element of the DPO role will be to advise the organisation how to make appropriate information available and accessible thereby facilitating the involvement process.

6. EQUALITIES IMPLICATIONS

6.1 An EIA screening has been completed in accordance with the Council's Strategic Equality Plan and supplementary guidance. No potential for unlawful discrimination and/or low level or minor negative impact has been identified, therefore a full EIA has not been carried out.

7. FINANCIAL IMPLICATIONS

7.1 None.

8. PERSONNEL IMPLICATIONS

8.1 The personnel implications are included in this report.

9. CONSULTATIONS

9.1 The report reflects the views expressed by the consultees.

10. RECOMMENDATIONS

10.1 It is recommended that Audit Committee endorse the proposal to add the DPO role to the responsibilities associated with Corporate Information Governance Manager post prior to an approval request being presented to Cabinet.

11. REASONS FOR THE RECOMMENDATIONS

11.1 The recommendation is compliant with the GDPR guidance available, ICO advisory publications and fits well with the current working practices and structure in place in CCBC.

11.2 The CIGM position already demands the technical knowledge required by GDPR and the associated DPO role. The current post-holder has an in-depth knowledge of CCBC's information holdings and strong working relationships with the service areas.

12. STATUTORY POWER

12.1 Local Government Act 2000.

Author: Paul Lewis, Acting Head of IT & Central Services and SIRO
E-mail: lewisps@caerphilly.gov.uk Tel: 01443 863267

Consultees: Cllr. Colin Gordon, Cabinet Member for Corporate Services
Cllr. Barbara Jones, Deputy Leader & Cabinet Member for Finance, Performance and Governance / Corporate Governance Panel Member
Richard Harris, Internal Audit Manager / Acting Deputy Monitoring Officer
Robert Hartshorn, Head of Policy and Public Protection / Corporate Governance Panel Member
Lynne Donovan, Acting Head of Human Resources and Organisational Development
Steve Harris, Interim Head of Corporate Finance
Lisa Lane, Corporate Solicitor
Bethan Manners, Senior Solicitor

Appendices:
Appendix 1 – Extract from GDPR (Articles 37, 38 and 39) on DPO role
Appendix 2 – Current Allocation of Data Protection Roles within the Council

APPENDIX 1

Extract from GDPR:

SECTION 4
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.

APPENDIX 2

Current Allocation of Data Protection Duties within the Council

1. The Data Controller for Data Protection purposes must be the Council, not an employee within the Council, but clearly this task must be delegated day to day. Due to legal changes over the last two decades, the Council has evolved a number of different reporting arrangements for Information Governance (IG), which encompasses data protection, broader information risk relating to non-personal information (e.g. confidentiality for drafts, commercial purposes, legal professional privilege, etc), records management and information requests. Allocation of the DPO role is an opportunity to review arrangements for information governance as a whole to achieve more consistency.

2. Currently the Council delegates data protection duties to the Senior Information Risk Owner (SIRO) (the Head of IT and Central Services), who manages 2.8 permanent and 1 temporary employee in the Corporate Information Governance Unit (CIGU) and oversees the Council's Information Governance Work Programme. The Corporate IG Manager deputises for the SIRO role when required. The SIRO reports to CMT via the Director of Corporate Services and Corporate Governance Panel have oversight of the Council's Information Governance Work Programme via regular reports. The Chief Executive decides on the majority of information request appeals, but the SIRO is responsible for data protection appeals and breaches.

3. To mitigate information risk whilst making better use of Council information assets, CIGU has devised a work programme for Information Governance Stewards Council-wide to advise their Service Area on routine data protection matters, information requests, records management and training requirements. More complex matters, exemptions, contracts, partnership arrangements, data breaches, etc are referred back to CIGU. IG Stewards undertake these tasks alongside their substantive post and whilst Directorates such as Education and Social Services have officers who are able to spend more time on these tasks, other Service Areas rely on a network of IG Liaison Officers to share the IG workload throughout their Service Area.

4. Legal impacts of IG proposals to reduce risk and make better use of information assets are considered by CIGU at Exemption Panel with the Head of Legal or Principal Solicitor and a representative from the Service Area. It is advantageous to have a distinction between IG and Legal Services, as compliance with law is one part of IG, but managing information to best practice standards to benefit service areas is equally important and the current Exemption Panel arrangements have proven to work very effectively over the last 12 years.

5. CIGU team members hold the nationally recognised ISEB qualification in Data Protection and the team has over 12 years experience of working with data protection legal changes, national case law, as well as experience of the Council, its services and its information assets. Retaining day-to-day tasks with this established team will satisfy the GDPR requirement for "professional experience and knowledge of data protection law that is proportionate to the level of protection that the personal data processed by the Council requires".

6. The SIRO role encompasses information risks across all types of information not just those records containing personal information and has a key role in advocating better ways of working to maximise use of the Council's information assets. Therefore it is desirable to maintain the SIRO role at a senior level to oversee Data Protection compliance as well as information risk more broadly, which also fits with best practice across the UK.

7. It is recommended that Information Governance remains a corporate function so that the Council as Data Controller can be assured that its information is managed consistently and risks are low across every Council service. Whilst other Service Areas are key stakeholders in information governance particularly if they process highly sensitive personal information, retaining the function within Corporate Services Directorate will provide corporate assurance and is consistent with the IG role in other local authorities.

8. The following arrangements have developed over time since DPA was passed in 1998 and FOI became fully implemented in 2005. Designation of the DPO role is also an opportunity to clarify responsibilities of the SIRO.

Role	History	Task
Senior Information Risk Owner (SIRO)	Cabinet Office recommended Board level role (one of key improvements after 2007 HMRC data loss). In Welsh LAs this role tends to sit with a Head of Service and in 2013 Audit Committee assigned the role to Head of IT and Central Services.	• Oversees info risk evidenced from six monthly info risk returns from each service. • Signs-off data breach outcomes and makes decision on self-reports to ICO. • Makes decisions on DPA complaints, including SARs. • Manages CIGU who undertake IG work day-to-day.
Chief Executive or other appropriate senior officer	CE assigned to review FOI/EIR appeals in 2004. Due to a number of instances where the CE had been involved in a situation that resulted in an FOI request, this was modified to "or an appropriate senior officer".	• FOI/EIR appeals
Exemption Panel	Originally established in 2005 for FOI/EIR exemptions, but quickly started to consider any IG matter that required a legal perspective (either a non-IG law impact on decision, or second opinion on an IG law that CIGU had researched).	• Comprises either Head of Legal or Principal Solicitor (on rota basis), CIGU rep and rep from Service Area. Decision is joint, but Exemption Form is signed by the solicitor on duty to give legal weight. • CIGU does background research on law, case law/decision notices and any guidance from regulators (ICO, Surveillance Commissioner, etc) and makes recommendation for Panel. • Consultee together with CIG Manager on FOI/EIR appeals prior to Chief Executive or appropriate senior officer making decision on outcome.
Data Protection Officer (statutory from May 2018)	This role has existed since early 1980s when DPA first introduced and sits with the Head of Service overall responsible for DPA compliance. Since 2013, DP Officer (Head of IT) has also been the SIRO, but the SIRO title has been used instead to reflect broader information risk associated with non-personal data and to fulfil the functions defined by Cabinet Office and WLGA recommendations.	• Currently same tasks as SIRO, as sits with same person. • Will be a statutory function from May 2018, which GDPR states needs to sit with someone with DPA expertise. • NB The corporate role needs to be called "Statutory" or "Corporate" DPO to avoid confusion with existing roles in Social Services Directorate.