GDPR Governance Structure

Introduction

In its response to the GDPR, the Council needs two governance structures. The first covering the period of the implementation project and the second for the post-implementation period to ensure high standards are maintained.

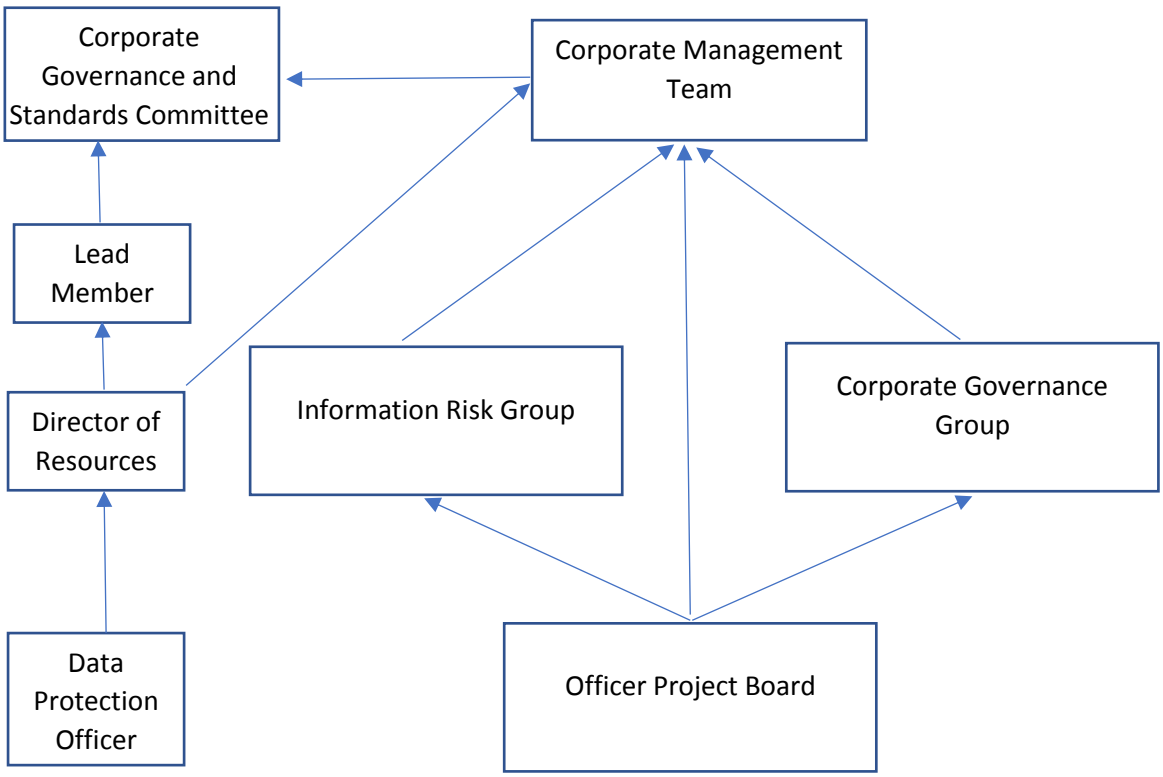
In both phases, there will be a prominent role for the Data Protection Officer (DPO). This is a role that the Council is required to introduce under the GDPR, in common with all public authorities.

Project Period

The governance objectives during this period will be to:

- ensure a successful implementation process so that the requirements of the GDPR are met by the deadline date of 25 May 2018 and
- provide assurance for the Corporate Management Team and Councillors regarding the progress of the implementation project.

The overall layout of the governance arrangements with the various groups and individuals involved is set out below. The diagram includes reporting lines.



The Council already has a structure of officer working groups responsible for the oversight of its governance arrangements. Ultimate responsibility for governance lies with the Corporate Management Team. However, there are two groups already in place to provide support and ongoing monitoring in this area; the Information Risk Group (IRG) and the Corporate Governance Group (CGG).

The Information Risk Group (IRG)
The IRG's role is to oversee the Council's response to all information risks. This includes Data Protection and covers Information Rights and the security of records. The group meets every 6 weeks and its members are:

- Director of Resources/Senior Information Risk Owner (SIRO)
- ICT Manager
- Information Rights Officer
- Chief Internal Auditor
- Principal Corporate Services Solicitor

The Corporate Governance Group (CGG)
The CGG monitors the Council's standards of governance, including information issues. The group meets quarterly and its members are:

- The Head of Paid Service
- Director of Resources
- Chief Finance Officer
- Monitoring Officer
- Deputy Monitoring Officers
- Principal Corporate Services Solicitor
- Democratic Services Manager

The Project Board
For the period of the project, there will be an Officers Project Board. The Board will meet monthly and be chaired by the DPO. The Director of Resources is the Project Sponsor and the Information Assurance Manager will be the Project Manager. The Board members will be:

- DPO (Chair)
- Information Assurance Manager (Project Manager)
- Communications Officer
- Directorate Representatives

The Officer Board will include at least one representative from each directorate. Ideally, these will be officers responsible for record management and/or the administration of the directorate's major systems.

During the project, the GDPR will be a standing item on Corporate Management Team (CMT) and directorate management team agendas. This will allow progress to be monitored at a service level and issues to be raised through departmental representatives to the Project Board.

The project will be managed through Verto (on-line project management resource). This will allow the Project Manager to produce standardised monitoring reports for the IRG, CGG and CMT. These reports will provide the opportunity for questions to be raised and concerns escalated to senior management and councillors where required.

Some group members are part of more than one group. Using Verto will avoid duplication of effort and ensure standardisation of reporting across the Council. The involvement of several groups allows issues and concerns to be addressed from different perspectives to ensure that all aspects are considered.

In addition to the formal group structure, there is a direct reporting line from the DPO, through the Director of Resources to the Lead Member and ultimately the Corporate Governance and Standards Committee. However, if the DPO or Director of Resources has concerns that they consider are not being addressed appropriately, they have authority to report directly to the CMT, the Lead Member or the Committee as appropriate.

While the DPO is not a statutory officer in the same way as the Monitoring Officer, Head of Paid Service or Chief Finance Officer, the role does have similar protections to those functions. Section 4 of the GDPR deals with the role and responsibilities of the DPO. Article 38, *Position of the Data Protection Officer* states that the DPO "shall not be dismissed or penalised by the controller or processor for performing his tasks".

The same section also requires that the DPO "shall directly report to the highest management level of the controller or processor".

The governance structure set out above satisfies these requirements.

Business as Usual

After the project is complete and following a successful transition period, the Council will enter the business as usual phase. The governance arrangements will be as those set out in the diagram above, with the exception that there would no longer be a Project Board.

The post of Information Assurance Manager will be a member of the IRG.

The DPO will monitor compliance with the GDPR, provide guidance and advice and act as the Council's contact point for the Information Commissioner's Office. The DPO will continue to provide reports to the CMT, IRG and CGG on a regular basis. These will cover the level of compliance with the Regulation and recommendations for improvements.

Some of the day-to-day work in relation to Data Protection will be undertaken by the Information Assurance Manager. In relation to Data Protection, the post-holder will work to standards set by the DPO and there is likely to be some cross-over between the activities of the DPO and the Information Assurance Manager. Certainly, the Information Assurance Manager will be required to provide technical support and advice to the DPO.

The Information Assurance Manager's substantive post is in ICT and their line manager is the ICT Manager. Appropriate liaison procedures will be established between the DPO and the ICT Manager to ensure that the Information Assurance Manager is able to dedicate enough time to their role in supporting the DPO.

The DPO will be the Council's Principal Corporate Services Solicitor, providing suitably independent scrutiny of those elements of data management and security that are the direct responsibility of ICT.

The GDPR also requires that there is no conflict of interest between a DPO's role regarding data protection and any other duties they may have. This precludes the DPO being a member of ICT. Appointing the Principal Corporate Services Solicitor as DPO satisfies this requirement.

It would not be appropriate for the SIRO to also be the DPO. The SIRO provides an independent oversight of the DPO. The Council's designated SIRO is the Director of Resources and Deputy Managing Director. The GDPR require that the DPO reports directly to the highest management level, which would preclude a member of CMT from being the DPO.

GDPR Action Plan: 12 Key Steps

Step 1: Awareness of the GDPR and its impact

To ensure decision makers and key people in the Council are aware the law is changing and to understand the impact this will have. Launch awareness campaign across the Council and establish a Project Board consisting of key stakeholders.

Step 2: Information we hold

Conduct an information audit. Document the personal data held by the Council, know where the data came from, also who the Council shares it with.

Step 3: Communicating privacy information

Review the Council's current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

Step 4: Individual's rights

Check Council procedures to ensure they cover all the rights individuals will have under the GDPR. For example procedures to cover how the Council would delete personal data or how the Council would provide data electronically and in a commonly used format.

Step 5: Subject Access Requests

Update the Council's procedures and plan how the Council will handle requests within the new timescales.

Step 6: Lawful basis for processing personal data

To identify the lawful basis for the Council's processing activity under the GDPR, to document that and update privacy notices to explain it.

Step 7: Consent

To review how the Council seeks, records and manages consent and decide whether any changes are required.

Step 8: Children

To consider whether the Council needs to put in place systems to verify an individual's age to obtain parental or guardian consent for any data processing activity.

Step 9: Data breaches

To ensure procedures are in place to detect, report and investigate a personal data breach.

Step 10: Data protection by design and Data Protection Impact Assessments (DPIA)

To work out how and when to implement data protection by design and DPIAs within the Council

Step 11: Data Protection Officers (DPO) To designate a DPO to monitor the Council's compliance with the GDPR.

Step 12: International To confirm whether the Council carries out any cross-border processing and if applicable determine the lead data protection supervisory authority.