Midlothian

Chief Internal Auditor
Jill Stacey

Audit Committee
Tuesday 12 March 2019
Item No: 5.4

Auditor: James Polanski, Ext 5646

Final Internal Audit Report

to

- **Chief Executive**
- **Directors**
- **Heads of Service,**
- **Legal Services Manager**
- **Information Governance/Security Services Lead**

on

Information Governance Framework and GDPR

22 February 2019

1 Introduction

1.1 The purpose of this audit was to review the Council's Information Governance Framework including roles and responsibilities, policy development, and implementation. This included a review of the Council's compliance with the requirements of the General Data Protection Regulations (GDPR).

1.2 The Data Protection Act 2018 (DPA) covers the use of personal data within the scope of the General Data Protection Regulation (GDPR) and beyond it. Amongst other provisions, it repeals and replaces the Data Protection Act 1998, incorporates the GDPR into UK law, lays the ground for free-flow of data between the United Kingdom and the European Union after the UK's withdrawal from the EU, sets out permitted exemptions under the GDPR, and sets out the duties and powers of the UK's Information Commissioner's Office (ICO).

1.3 The Data Protection Act 2018 was given Royal Assent on 23 May 2018, and GDPR came into force from 25 May 2018.

1.4 GDPR provides individuals with more power and control over their personal data by strengthening and unifying data protection for all EU individuals with more rights and control over how their personal data is handled by organisations such as the Council.

2 Audit Scope

2.1 The scope of this audit was to examine and evaluate the following areas:

- the information governance policies and procedures established by the Council; and
- the controls in place to monitor compliance with the Council's information governance policies and procedures.

3 Management Summary

Information Governance Policies

3.1 The GDPR requires organisations to demonstrate how they comply with the principles. Midlothian Council has an approved Privacy Policy in place (approved by CMT November 2017). The principles of GDPR are adequately outlined in the policy, as are the roles and responsibilities of the Council and key staff members.

3.2 The GDPR requires that all public authorities appoint a Data Protection Officer (DPO), an officer with responsibility for the organisation's data protection compliance. In May 2018, CMT appointed the Legal Services Manager to act as the DPO on a short term basis until a full time DPO is appointed, with the Principal Solicitors as Depute DPOs to ensure business continuity and resilience in the absence of the DPO. At the time of reporting, interviews for the DPO role had been undertaken in late January 2019, and the DPO will soon be appointed.

3.3 It is mandatory for the Council to register with the ICO and pay the associated data protection fee. This was verified through review of the ICO register and the payment made to ICO through review of the record in the Council's finance system.

3.4 The Council has an Information Security Policy in place, available on the Council's Intranet, and it has been recently updated for GDPR. No issues were noted with the policy. Additionally, comprehensive written procedures and guidance documents are easily accessible on the Council's Intranet Information Management page. The procedures cover many information management topics.

3.5 Article 5(1)(e) of the GDPR requires that data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. The Council has a comprehensive data retention schedule in place that is easily accessible for all employees. Within the register it includes the reasoning for the retention of the data (business requirement, legal, or best practice), and no issues were noted with the time period or reasoning as described. An approved Records Management Policy is in place, available on the Council's Intranet Business Services page, and the policy has been updated for GDPR. Records Management will be subject to a separate review on Information Governance next year.

3.6 Further work is required to prepare the Individual Rights Policy (referenced to as an appendix within the Privacy Policy), which would define individual's rights in further detail and how the Council manages these rights, including Subject Access Requests which are referred to later in this report. The Privacy Policy also refers to an Open Data Strategy as an appendix. It is understood that this area of work is outstanding to address how to make public service and commercial data openly available for everyone to use and republish as they wish. Furthermore the Council does not yet have a Data Quality policy which provides an overarching, corporate approach to the management of data quality to support decision making, and helps demonstrate the accountability principle of the GDPR.

Information Asset Register and Data Protection Impact Assessments

3.7 Article 30 of GDPR requires that each controller shall maintain a record of processing activities under its responsibility. Compliance with this Article is achieved through an Information Asset Register (IAR). The GDPR Project Team developed the IAR template and guidance on how to complete the IAR, and provided support to Services for completion of the IARs. Review of the template noted it covered the mandatory requirements of Article 30, and this can be further developed over time to go into the level of detail described by ICO as 'best practice'.

3.8 The Council has acquired a system called OneTrust to record details of all the Council's information assets. This software will allow Services to periodically update their register, and email reminders can be sent directly to the relevant officers. Review of the Council's IARs identified that almost all Services had completed their IAR, with 3 minor exceptions.

3.9 It was noted that further work is required in establishing if the information sharing agreements documented in the IAR have been updated for GDPR, and if additional information sharing agreements are required for any gaps identified though the Services' completion of the IAR, as well as quality assurance of IAR responses (legal basis).

3.10 GDPR has introduced a legal requirement to carry out a data protection impact assessment (DPIA) for any type of processing that is likely to result in a high risk to the rights and freedoms of individuals. DPIAs help organisations identify the most effective way to comply with data protection obligations (privacy by design) and meet individuals' expectations of privacy. DPIA guidance and a template have been published on the Council's Intranet Information Management page, and training has been provided to relevant officers. The template and guidance was reviewed and no issues were noted.

3.11 The activity is work in progress with the intention for Managers to record DPIA completion via self-service through the OneTrust Information Asset Register as the central register of DPIAs.

Privacy Notices and Forms

3.12 In accordance with GDPR Article 13, where personal data relating to a data subject is collected, the Council uses privacy notices to: explain the purposes of processing; the legal basis for processing; the data subjects rights in relation to their personal data held by the Council; whether the data will be shared with any other parties; whether there is any automated decision making or profiling using the personal data; the retention period; and the contact details of the Data Protection Officer, responsible for monitoring the Council's compliance with Data Protection legislation.

3.13 The GDPR project team, through the IAR process, helped Services develop Privacy Notices that adequately describe their activities. A sample of 10 Privacy Notices were reviewed as part of this audit, and no issues were noted. A sample of 20 paper forms and 15 online forms were selected to check whether they included the relevant Data Protection Act 2018 wording which identified that not all had been appropriately updated. Discussion with the Performance Officers identified that work has been underway to ensure that Service's forms are being updated to include the relevant privacy notice wording.

Freedom of Information Requests and Subject Access Requests

3.14 The public are entitled to make requests for information held by the Council under the Freedom of Information (Scotland) Act 2002 (FOI). The Council has an FOI system in place with nominated, trained, FOI contacts who take forward the FOI requests. Comprehensive guidance documents for this are available on the Council's Intranet FOI page.

3.15 The Council's process on Subject Access Requests (SAR) was discussed with the three directorate Performance Officers as part of this audit. It was noted that the Performance Officers were knowledgeable of the requirements of the SAR process, and no issues were noted.

3.16 Metrics on FOIs and SARs are reported to the IMG and CMT on a regular basis for monitoring of the Council's compliance in meeting the statutory response times and taking action as appropriate. These are important indicators, as continued late responses could result in a fine from ICO. There has been a noticeable increase in the volume of SARs received by the Council, which presents a challenge due to complexity of some of the requests and response timescales. It is noted that some Councils publicly report on their performance in responding to SARs and FOIs within the statutory response times, a practice not currently adopted by Midlothian Council.

Data Breaches

3.17 The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. This must be done within 72 hours of becoming aware of the breach, where feasible. The IMG has established a procedure for reporting data breaches and reviewing security incidents. Any lessons learned and ICO recommendations, where relevant, are considered and implemented as appropriate.

3.18 The importance of reporting Data Breaches to the IMG contacts has been highlighted to staff through the mandatory training, Management, and periodic notifications from the IMG via email and the staff magazine. The Data Breach procedure was reviewed, and no issues were noted with the procedure.

Training

3.19 Staff training is an essential part of GDPR compliance. Staff training reduces the risk of errors, inconsistencies, and data breaches. Additionally, it helps demonstrate compliance with GDPR (the Accountability Principle).

3.20 Prior to the introduction of GDPR, the Council arranged training sessions for second and third tier managers and other key staff to ensure that they are aware of GDPR's requirements and to assess the impact this would have on their Services. A mandatory GDPR training module has been made available to all staff on the LearnPro e-learning system. Additionally, measures have been taken to ensure employees who do not have access to a computer complete the training module. The ICO expects organisations to evidence a 95% completion rate.

3.21 The take-up of the training module (including employees who do not have access to a computer) as at 31/01/2019 is as follows:

Directorate	Percentage Complete
Elected Members	20.00%
Education, Communities and Economy	74.22%
Health and Social Care	72.83%
Resources	52.10%
Total	65.49%

3.22 Completion rates for the GDPR mandatory training are reported to the IMG and CMT on a regular basis, and reminders have been issued to staff by Management to encourage completion across the Directorates.

3.23 Officers have advised that further specialist GDPR training will be rolled out in 2019 to ensure all employees are appropriately trained and further demonstrate compliance with GDPR.

Compliance Monitoring

3.24 The Council has an Information Management Group (IMG) in place, with an appropriate Terms of Reference. The remit of the IMG is to identify and maintain high quality information assets and to share these assets in accordance with current data protection legislation and best practice. It was noted that the IMG meets regularly, appropriately reviews and monitors the Council's activities relating to data and data protection, and periodically reports the findings of the Group, including progress with implementing the requirements of the GDPR, to Senior Management.

3.25 The ICO controller's checklist recommends that organisations should establish a formal process of self-assessing compliance with GDPR (section 3.1 of the controller's checklist). This includes testing measures within the policies to provide assurances about their continued effectiveness. The Council does not yet have a formal self-assessment process in place, but is understood from discussion with Management that this will be introduced once the new DPO is in post.

Assurance Opinion

3.26 We consider that we are able to provide substantial assurance. Largely satisfactory risk, control, and governance systems are in place. There is, however, scope for improvement as current arrangements could undermine the achievement of objectives. This includes, ensuring that there is adequate quality assurance work carried out on the Information Asset Register and evaluation of Service responses, review of all Information Sharing Agreements to ensure compliance with GDPR and sufficiency of the agreements, further roll out of GDPR training, and ensuring all relevant forms have been updated for GDPR. Management actions are underway to address areas of known risk, as has been recently reported to the Corporate Management Team.

3.27 Further best practice improvements were identified in this review such as ensuring completion of policies supporting the Privacy Policy (Individual Rights Policy, Data Quality Policy, and Open Data Strategy), implementation of a data protection self-assessment process as recommended by ICO, and improvements in reporting of SARs and FOIs.

3.28 In light of this review and the Council's Internal Audit Strategy reference to its 'critical friend' role, it is proposed that an Internal Auditor joins the Council's Information Management Group as a virtual member and attends meetings quarterly, as this will allow monitoring of completion of any improvement actions being progressed by Management as part of continuous auditing.

3.29 The Internal Audit function conforms with the professional standards as set out in the Public Sector Internal Audit Standards (2017), including the production of this report to communicate the results of the review. We would like to thank those officers who assisted us during our review.