Internal Audit Report
Corporate & Democratic Service
General Data Protection Regulation
Assignment No 18-21
March 2019 (Report No.19/99)

Final Report

Legal and Governance
Corporate and Democratic Services
Perth & Kinross Council
Council Offices
2 High Street
Perth
PH1 5PH

Internal Audit

"Internal Audit is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes". Public Sector Internal Auditing Standards (PSIAS)

The Council's Audit Committee approved the PSIAS as the relevant standard for its Internal Audit activity.

Background and Introduction

This audit was carried out as part of the audit plan for 2018/19, which was approved by the Audit Committee on 27th June 2018. Audit testing was carried out in January and February 2019.

The General Data Protection Regulation [GDPR] has been effective since May 2018 and introduces changes to the 1998 Data Protection Act regarding controls on personal information. There is a new principle of accountability and increased penalties can be incurred for non-compliance. The Regulation is designed to protect individuals when their personal data is processed. The Data Protection Act 2018 sits alongside the GDPR for its implementation in the UK. Data Protection is generally included, not GDPR specifically, in the Council's risk register as a strategic risk on arrangements to prevent the Council from keeping our data safe and secure.

The GDPR introduces a duty for public authorities, including the Council, to appoint a Data Protection Officer (DPO). It details the DPO's tasks and places restrictions on the position and this is supplemented by guidance from the Information Commissioner's Office. As a controller, the Council is responsible and accountable for processing personal information. Likewise, when the Council shares personal information with its partner organisations, this should be clearly indicated at the point of collecting the personal information.

Scope and Limitations

Key officers interviewed during the review included the Council's Information Governance Manager and Records Manager, the Procurement Manager and key Officers for Data Protection in Education and Children's Services. A review of evidence on the Information Governance Group site was also undertaken.

Control Objectives and Opinions

This section describes the purpose of the audit and summarises the results. A 'control objective' is a management objective that requires the maintenance of adequate and effective internal controls to ensure that it is achieved. Each control objective has been given a rating describing, on the basis of the audit work done, the actual strength of the internal controls found to be in place. Areas of good or poor practice are described where appropriate.

Control Objective: To ensure that Council is progressing with compliance to the new GDPR requirements

Internal Audit Comments:

The Council has a designated Data Protection Officer [DPO], named with contact details provided to the Information Commissioner's Office, recorded on the Council's website and accessible to all. The DPO is the Council's Information Governance Manager, who also acts as the Records Manager, and has a Team resource to assist. The DPO has independence in that the GDPR largely defines their job role, not the Council. The DPO reports to the Council's Head of Legal & Governance as Line Manager, but has access to the Corporate Management Team, the Chief Executive and Executive Officer Team. He has a responsibility for reporting on GDPR compliance to the Executive Officer Team and the Scrutiny Committee at least annually. As it is the first year of GDPR implementation, reporting is planned to take place to the end of March 2019, to be reported in June; discussions between the DPO and the Head of Legal & Governance have been held towards implementing this.

The GDPR requires the Council to have a Statement of Policy. This has been done and sits within the Data Protection Policy, approved by Strategic Policy & Resources Committee in November 2018. There are no specific responsible persons/job roles named and responsibility falls on all in the Council.

This Policy defines the roles and responsibilities of others, including Head of Legal & Governance Services, Service Senior Management Teams, Elected Members, employees, agents and volunteers.

The Policy states that Council Services will identify Lead Officers for Data Protection and meet regularly. In December 2018 the first Data Protection Group meeting was attended by 14 Service representatives, including people who had worked on the previous GDPR Implementation Group until August 2018.

The Corporate and Democratic Services' Business and Management Improvement Plan 2018-2021 has an action to review and revise all policies, processes and procedures in relation to the Council's processing of personal information with a target date for completion by Summer 2019.

The Council has a Register of Processing Activities as required by GDPR. Processing activities listed on the Register during the audit review numbered 43 for Education & Children's Services; 190 for Corporate & Democratic Services; 188 for Housing & Environment; and 29 for Adult Social Care. Work on this register is still progressing. To make clear the legal basis of processing personal data, the Council publishes detailed Privacy Notices on its website with contact details if more information is wanted. When systems or processes which handle personal data are changed or new ones introduced, Data Protection Impact Assessments are carried out in compliance with the GDPR.

Under the GDPR, contracts with suppliers involving personal data should contain clauses defining data protection responsibilities. The Terms and Conditions in Council standard contracts were reviewed and amended to incorporate provisions relevant to the GDPR. This included a 'future proofing' variation clause to enable amendments to incorporate future amends to the Data Protection Laws (including the Data Protection Act 2018 which supplemented GDPR).

The Register of Processing Activities has to record data sharing: it currently lists 23 activities involving data sharing. The Council names 13 organisations it mainly

shares information with on its website and provides the contact details of the DPO for more details as required. In addition, the DPO has a record of 27 completed data sharing agreements by Service, with the status showing more in progress. A template data sharing agreement is available and the DPO offers consultation for Services to complete these. In the event of a data breach occurring, the Data Protection Policy requires these to be reported to the DPO to investigate and manage, dependent on the circumstances of the breach type and severity. Council officers have been reminded by bulletins on Eric of what to do in the event of a suspected breach, the importance of reporting these timeously, common breach areas and how to avoid these. It is noted that in the event of a breach, the Information Commissioners Office (ICO) has always asked about the staff training of the individuals concerned. A review in Education & Children's Services found evidence of ECS officers moving GDPR forward, through ECS newsletters, presentations by the DPO and bulletins to all Head Teachers at their conference days in 2018. ECS Research and Performance Team Manager confirmed GDPR training was rolled out to school staff through the Local Management Group meetings.	
Strength of Internal Controls:	Moderately Strong

Management Action and Follow-Up

Responsibility for the maintenance of adequate and effective internal controls rests with management.

Where the audit has identified areas where a response by management is required, these are listed in Appendix 1, along with an indication of the importance of each 'action point'. Appendix 2 describes these action points in more detail, and records the action plan that has been developed by management in response to each point.

It is management's responsibility to ensure that the action plan presented in this report is achievable and appropriate to the circumstances. Where a decision is taken not to act in response to this report, it is the responsibility of management to assess and accept the risks arising from non-implementation.

Achievement of the action plan is monitored through Internal Audit's 'follow up' arrangements.

Management should ensure that the relevant risk profiles are reviewed and updated where necessary to take account of the contents of Internal Audit reports. The completeness of risk profiles will be examined as part of Internal Audit's normal planned work.

Acknowledgements

Internal Audit acknowledges with thanks the co-operation of Council Officers during this audit.

Feedback

Internal Audit welcomes feedback, in connection with this audit or with the Internal Audit service in general.

Distribution

This report has been distributed to:

K Reid, Chief Executive

J Valentine, Depute Chief Executive (Chief Operating Officer)

L Simpson, Head of Legal and Governance, CADS

D Henderson, Information Governance Manager, CADS

M Mitchell, Corporate Procurement Manager, CADS

P Davison, Corporate Research and Information Manager, ECS

Committee Services

External Audit

Authorisation

The auditor for this assignment was N Duncan. The supervising auditor was M Morrison.

This report is authorised for issue:

_____

J Clark
Chief Internal Auditor
Date: 15 March 2019

Appendix 1: Summary of Action Points

No.	Action Point	Risk/Importance
1	Services Lead Officers for Data Protection	Low
2	Privacy Notices and Data Protection Impact Assessments	Medium
3	Contracts and Data Sharing Agreements	Medium
4	Training, guidance and uptake	Medium

Appendix 2: Action Plan

Action Point 1 - Services Lead Officers for Data Protection

The Data Protection Policy refers under Governance to Services identifying Lead Data Protection Officers. These Lead Officers are to meet regularly with the Council's DPO to consider Data Protection practice and procedures.

The first Data Protection Group meeting was held in December 2018 with the DPO and 14 officers representing most Services. More quarterly meetings were planned to follow.

Management Action Plan

At a future Data Protection Group meeting in 2019 discussion and agreement on roles of Data Protection Lead Officers for each Service to be moved forward towards compliance to the Council's Data Protection policy.

Risk/Importance:	Low
Responsible Officer:	D Henderson, Data Protection Officer
Lead Service:	Corporate & Democratic Services
Date for Completion (Month / Year):	December 2019
Required Evidence of Completion:	Minutes of Meeting

Auditor's Comments

Satisfactory

Action Point 2 - Privacy Notices and Data Protection Impact Assessments

The Council provides privacy information towards compliance to new GDPR standards. In addition to the high level Privacy Notice published on the Council website, other detailed Privacy Notices are also published for specific processes involving personal data. Twenty five were available, with contact details of the Information Governance Team for further details as required. Template Privacy Notice documents are available from the Team and are published on Eric. More Service specific Privacy Notices require to be completed to match the number of processing activities listed on the Register of Processing Activities.

Data Protection Impact Assessments are a mandatory requirement of GDPR when new systems are introduced or when processes which handle personal data are changed. The DPO has provided a template towards assisting Council Services complete these. A review of Data Protection Impact Assessments on the shared Information Governance Group site found that 85 were listed for all Council services, of which 16 had been approved by the asset owner, 40 were in progress and 29 had other statuses.

Management Action Plan

The DPO will continue to liaise with Services to ensure that all Privacy Notices listed on the Register of Processing Activities and Data Protection Impact Assessments have been completed, as recources allow.

Risk/Importance:	Medium
Responsible Officers:	D Henderson, Data Protection Officer
Lead Service:	Corporate & Democratic Services
Date for Completion (Month / Year):	December 2019
Required Evidence of Completion:	Update on the number of Data Protection Impact Assessments progressed

Auditor's Comments

Satisfactory

Action Point 3 - Contracts and Data Sharing Agreements

a) When contracts were assessed for risk of non-compliance to GDPR prior to implementation in 2017, there were approximately 500 potential suppliers with 700 contracts which may involve personal data. The Procurement Manager reported that the risk of non-compliance with GDPR for contracts has since reduced due to the renewal of transport contracts, which have an element of personal data, in 2018. However there is a residual risk from contracts such as IT suppliers which still have to be identified and managed. This risk review is an action planned for 2019 by the Procurement Manager.

b) The Council's Contract Rules 2017 are due for review in Sept 2019. The Section 8 Legal Framework does not have specific mention of Data Protection legislation. The general statement 'Every contract must comply with all relevant legislation' is included in section 8 – Legal Framework as a 'catch-all' statement.

c) The DPO reported that Services are signing off draft Data Sharing Agreements before being reviewed by the DPO.

Management Action Plan

a) Procurement to identify most likely contracts involving processing of personal data and contract owners to be notified of GDPR contract requirements [with advice from DPO].

b) The PKC Contract Rules review to consider specific requirements for GDPR in section 8 – Legal Framework.

c) Services to be reminded of the need for the DPO to have sight and review of draft for Data Sharing Agreements before final sign off as set out in Council policy.

Risk/Importance:	Medium
Responsible Officers:	a) M Mitchell, Procurement Manager b) M Mitchell, Procurement Manager c) D Henderson, Data Protection Officer
Lead Service:	Corporate & Democratic Services
Dates for Completion (Month / Year):	a) May 2019 b) September 2019 c) March 2019
Required Evidence of Completion:	a) Copy of communication b) Confirmation that a review has taken place and evidence thereof c) Copy of communication

Auditor's Comments

Satisfactory

Action Point 4 - Training, Guidance and Uptake

GDPR training is available for users with access to the online platform Learn, Innovate, Grow and GDPR training is mandatory. There were also Learning Lunches, updates on Eric and presentations to Service staff and staff groups. Training areas included for example, Data Protection Impact Assessments, common breaches and how to reduce these occurring.

Across all Council Services, the up-take figures for the latest GDPR on-line training to Feb 2019 showed 373 had completed the GDPR.

This suggests that not all users have completed mandatory GDPR training. It was reported that when there is a breach the ICO always request information about staff training.

Management Action Plan

a) Further reminders to staff with links to the training updates continuing to promote the need and uptake of GDPR training, with clear message that this is mandatory.

b) As part of a review into the Council's approach to encouraging people to undertake training and development, arrangements will be put in place to ensure that managers are aware of what essential training is required to be undertaken by their teams

Risk/Importance:	Medium
Responsible Officer:	a) D Henderson, Data Protection Officer b) S Flanigan, Corporate Strategy and Organisational Development Manager
Lead Service:	Corporate & Democratic Services
Date for Completion (Month / Year):	a) June 2019 b) August 2019
Required Evidence of Completion:	a) Copy of communication b) Outcome from review and communication with managers

Auditor's Comments

Satisfactory