Argyll & Bute Council - Internal Audit Report

June 2018

Final

General Data Protection Regulations

Audit Opinion: Substantial

	High	Medium	Low
Number of Findings	**0**	**1**	**0**

Contents

Contact Details

Internal Auditor: ***David Sullivan***

Telephone: ***01546 604125***

e-mail: ***david.sullivan@argyll-bute.gov.uk***

1. Executive Summary

Introduction

1. As part of the 2018/19 internal audit plan, approved by the Audit & Scrutiny Committee in March 2018, we have undertaken an audit of Argyll & Bute Council's (the Council) system of internal control and governance in relation to General Data Protection Regulations (GDPR).

2. The audit was conducted in accordance with the Public Sector Internal Audit Standards (PSIAS) with our conclusions based on discussions with council officers and the information available at the time the fieldwork was performed.

3. The contents of this report have been agreed with the appropriate council officers to confirm factual accuracy and we would like to record our appreciation for the cooperation and assistance we received from all officers over the course of the audit.

Background

4. The EU legislation 2016/679 GDPR provides individuals with more power and control over their personal data by strengthening and unifying data protection for all EU individuals and more rights and control over how their personal data is handled by organisations such as the Council. The main changes are:

   Consent: The conditions for consent have been strengthened, and organisations must use consent requests which are clear and plain. It must be also be made as easy to withdraw consent as it is to give it.

   Breach Notification: Breach notification is mandatory where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach.

   Right to Access: Data subjects have the right to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose.

   Right to be forgotten: This entitles the data subject to have their personal data erased, cease further dissemination of the data, and potentially have third parties halt processing of the data. The exceptions to this right are if the personal data belonging to the data subject is related to the delivery of a statutory service or to prospective legal claims.

   Data Portability: Data portability is the right for a data subject to receive the personal data concerning them, which they have previously provided, in a "commonly used and machine readable format" and have the right to transmit that data to another controller.

   Privacy by Design: Privacy by design requires the inclusion of data protection from the onset of the design of systems or process, rather than as an addition. This means the Council needs to consider data protection at the beginning and throughout the design process.

   Penalties: Under GDPR organisations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements, e.g. not having sufficient customer consent to process data or violating the Privacy by Design concepts. There is a tiered approach to fines, e.g. an organisation

can be fined 2% for not having their records in order, not notifying the supervising authority and data subject about a breach or not conducting an impact assessment. A fine of this level would have a major impact on service delivery.

5. The GDPR is in force from 25 May 2018 and the Data Protection Act 2018 was given Royal Assent on 23 May 2018

Scope

6. The scope of the audit was to ensure that appropriate governance and procedures are in place to ensure the Council will comply with the requirements of GDPR.

Audit Opinion

7. We provide an overall audit opinion for all the audits we conduct. This is based on our judgement on the level of assurance which we can take over the established internal controls, governance and management of risk as evidenced by our audit work. Full details of the five possible categories of audit opinion are provided in Appendix 2 to this report.

8. Our overall audit opinion for this audit is that we can take a **substantial** level of assurance. This means that internal control, governance and the management of risk are broadly sound. However, there are minor areas of weakness which put some system objectives at risk and specific elements of residual risk that are slightly above an acceptable level and need to be addressed within a reasonable timescale.

Key Findings

9. We have highlighted one medium priority where we believe there is scope to strengthen the control and governance environment. This is summarised below:

    - Action should be taken to ensure mandatory GDPR training is carried out by all relevant staff.

10. Full details of the audit findings, recommendations and management responses can be found in Section 3 of this report and in the action plan at Appendix 1.

2. Objectives and Summary Assessment

11. Exhibit 1 sets out the control objectives identified during the planning phase of the audit and our assessment against each objective.

Exhibit 1 – Summary Assessment of Control Objectives

	Control Objective	Assessment	Summary Conclusion
1	There is appropriate governance in place to effectively manage the activity required to ensure GDPR compliance.	Substantial	There is clarity over responsibility for ensuring GDPR compliance with appropriate progress monitoring and reporting in place. The project was monitored via a Project Implementation Plan (PIP) which covered the main tasks required for compliance. Council staff have been informed of the key features of GDPR via the HUB and a GDPR training module is available on LEON however the uptake of this training needs to be improved.

2	Satisfactory progress is being made to ensure the Council has appropriate procedures in place to ensure GDPR compliance.	Substantial	Appropriate procedures have been prepared and forwarded to the relevant personnel which cover all areas of GDPR in order to ensure compliance. A total of 80 privacy notices covering all Council services have been prepared and checked, of which 72 are on the website. The remaining eight are subject to final check before inclusion on the website.
3	The Council has a GDPR risk register in place.	Substantial	The implementation of GDPR, and its associated risks is included in the Governance and Law risk register. Heads of service have been requested to consider adding a GDPR risk to their register.

12. Further details of our conclusions against each control objective can be found in Section 3 of this report.

3. Detailed Findings

There is appropriate governance in place to effectively manage the activity required to ensure GDPR compliance

13. The Governance and Law service is responsible for managing the project to ensure the GDPR compliance. To deliver the project the Governance & Risk Manager (G&RM) is supported by resources from Legal Services and a Special Projects Officer. As required by GDPR the Council have appointed a Data Protection Officer. This role is assigned to the G&RM.

14. The G&RM chairs the Council's Information Security Forum (ISF) with members of the ISF acting as lead officers who liaise with services to provide support and guidance to prepare for GDPR. The ISF meets regularly and it is clear that it gives appropriate attention to GDPR compliance.

15. The project is managed using a PIP which covers the main tasks required to ensure compliance with GDPR including due dates, a traffic light status and a comments section. Progress against the PIP is regularly reported to the Senior Management Team (SMT) and ISF via regular reports provided by the project team.

16. Key information on GDPR has been made available to employees via the Council HUB and a training course is available via the Council's online training module LEON. The course has been classified as mandatory for all staff who deal with personal data with a completion deadline of 31 May 2018. As at 31 May 2018, 2,366 members of staff have completed the course. This is 56% of staff. A number of staff have restricted or no access to the LEON module, mainly manual workers, home helps etc. and guidance has been issued to the ISF reps to forward to appropriate managers to cascade the guidance to those staff groups. The list of staff on the LEON database included names of some staff that had left the organisation and the names of staff without network access, therefore the figure of 56% is likely to be higher.

Action Plan 1

Satisfactory progress is being made to ensure the Council has appropriate procedures in place to ensure GDPR compliance

17. GDPR requires the Council to document the personal data it holds, where it came from and who they share it with. Each service already has an Information Asser Register (IAR) that summarises the data they hold across various IT platforms. Guidance was issued that outlined what additional information should be included in these IARs to address GDPR compliance and all IAR's are compliant. It should be noted the IAR's are 'live' documents and will require ongoing review in regard to Records Management requirements.

18. The Council are required to supply data subjects with information, such as the requirement to explain the lawful basis for processing their data, data retention periods and the right to complain to the Information Commissioner Officer (ICO) if they are concerned about the manner in which the Council is handling their data. The ICO recommend that this information is provided via a privacy notice. There is guidance outlining the various scenarios where the Council can legally process an individual's data and also guidance for services to enable them to prepare the privacy notices. All privacy notices highlighted by the IAR review have been completed.

19. The Council had a requirement to prepare a total of 80 privacy notices across all services and 72 are on the website and eight are going through the final check before being passed to the web team for inclusion on the website.

20. GDPR sets out the various rights that individuals will now have and they have been included in the privacy notices with fuller details on the website. These include the right:

    - to be informed of data held
    - of access to data
    - to rectification of data
    - to erasure of data
    - to restrict processing
    - to data portability
    - to object to data held.

21. The Council needs to have procedures to manage enquiries from individuals about the personal data the Council may hold on them. Information is available to members of the public on their rights and the subject access request process on the website and guidance has been issued to staff on their role if they receive a subject access request, this is available on the HUB and information has been issued via a newsflash.

22. The Council needs to have a procedure enabling individuals to grant consent to process their data. The project team have provided assurances that the Council will not require individual consent for the delivery of the majority of Council services. Instead each privacy notice outlines the legal basis, as defined by the legislation, by which the Council will provide the service e.g. on a statutory basis in terms of the Education (Scotland) Act 1980 or Social Work (Scotland) Act 1968 or to carry out a task in the public interest or in terms of a contract. Areas where consent is currently held is considered as being compliant with the requirements of the new legislation, however, the ICO has recommended that there should be a systematic review of the procedures for obtaining consent to ensure future compliance. A briefing note, checklist and template relating to consent has been made available on the ISF SharePoint site and have also been issued to services and made available on the Data Protection page on the HUB.

23. In compliance with GDPR the Council has prepared a comprehensive data breach procedure document which defines the type of incident that would qualify as a data breach, who is responsible for reporting it, who it should be reported to and the reporting timescale.

24. The Council are required to consider data protection and privacy in the early stages of any project and throughout its lifecycle. E.g. when developing new information technology systems, developing policy or strategies or when embarking on a data sharing initiative. The project team has prepared a guidance note entitled "Privacy by Design and Data Protection Impact Assessment" which is available on the HUB and information advising staff has been included in the newsflash.

25. GDPR requires the Council to have data sharing arrangements with services internal to the Council and also external organisations. The project team have confirmed that work on data sharing agreements is being carried out in conjunction with procurement who are implementing amendments to current contracts to incorporate data processing agreements. Procurement agreements post 25 May 2018 will reflect the requirements of the GDPR and the Data Protection Act 2018.

The Council has a GDPR risk register in place

26. The implementation of GDPR, and its associated risks should feature in the operational risk registers for all services across the Council and a request has been sent to Heads of Service asking them to consider adding a risk to their register. The Governance and Law register includes the risk.

Appendix 1 – Action Plan

	No.	Finding	Risk	Agreed Action	Responsibility / Due Date
Medium	1	**Completion of GDPR Training** A GDPR training module has been made available on LEON and is classified as mandatory for all staff who deal with personal data. A completion deadline of 31 May 2018 has been set. As at 21 May 2,366 members of staff have completed the course. This is 56% of staff.	Staff are not appropriately aware of GDPR requirements and what is required of them to ensure Council compliance.	Project team will remind Heads of Service by e-mail that relevant staff should complete LEON training module. In addition further guidance to non-network personnel on how they could access and complete the LEON module will be provided	Governance and Risk Manager 30 June 2018

In order to assist management in using our reports a system of grading audit findings has been adopted to allow the significance of findings to be ascertained. The definitions of each classification are as follows:

Grading	Definition
High	A major observation on high level controls and other important internal controls or a significant matter relating to the critical success of the objectives of the system. The weakness may therefore give rise to loss or error.
Medium	Observations on less significant internal controls and/or improvements to the efficiency and effectiveness of controls which will assist in meeting the objectives of the system. The weakness is not necessarily substantial however the risk of error would be significantly reduced if corrective action was taken.

Low	Minor recommendations to improve the efficiency and effectiveness of controls or an isolated issue subsequently corrected. The weakness does not appear to significantly affect the ability of the system to meet its objectives.

Appendix 2 – Audit Opinion

Level of Assurance	Definition
High	Internal control, governance and the management of risk are at a high standard. Only marginal elements of residual risk have been identified with these either being accepted or dealt with. A sound system of control designed to achieve the system objectives is in place and being applied consistently.
Substantial	Internal control, governance and the management of risk is sound. However, there are minor areas of weakness which put some system objectives at risk and specific elements of residual risk that are slightly above an acceptable level and need to be addressed within a reasonable timescale.
Reasonable	Internal control, governance and the management of risk are broadly reliable. However, whilst not displaying a general trend, there are a number of areas of concern which have been identified where elements of residual risk or weakness may put some of the system objectives at risk.
Limited	Internal control, governance and the management of risk are displaying a general trend of unacceptable residual risk above an acceptable level and placing system objectives are at risk. Weakness must be addressed with a reasonable timescale with management allocating appropriate resources to the issues raised.
No Assurance	Internal control, governance and the management of risk is poor. Significant residual risk and/or significant non-compliance with basic controls exists leaving the system open to error, loss or abuse. Residual risk must be addressed immediately with management allocating appropriate resources to the issues.