AUDIT REPORT 23'015

UK GENERAL DATA PROTECTION REGULATION

Executive Summary

The annual internal audit plan for 2022/23 provides for a review to be undertaken of the Council systems to ensure compliance with United Kingdom's (UK) General Data Protection Regulation. The General Data Protection Regulation (GDPR) was a 2016 European Union regulation that came into force in May 2018, at the same time as the UK's updated Data Protection Act 2018 (DPA). Since the UK's departure from the European Union, GDPR has been adopted into UK regulation and sits alongside DPA 2018; together they introduce stronger legislation on the handling of personal data.

The Council processes an individual's personal data in order to plan, run and improve its services, perform its statutory duties, carry out its regulatory, licensing and enforcement roles, make payments, administer benefits and identify fraud and improve the health of the population it serves. The UK General Data Protection Regulation regulates and protects the processing of personal data about individuals by using the law to protect data and the way it is used by Local Authorities.

The scope of the audit reviewed systems and controls to ensure the Council is fulfilling the requirements of UK GDPR. The review sought to confirm the required policies, procedures and guidance are in place, there is awareness throughout the Council with comprehensive training programmes and effective oversight and governance arrangements to monitor ongoing compliance with UK GDPR. Failures that result in a breach of an individual's personal data may result in the Information Commissioner's Office issuing a fine to the Council.

The audit was carried out in accordance with Public Sector Internal Audit Standards (PSIAS).

Difficulties were experienced during the audit in the provision of information required for this review. This resulted in a delay in the completion of the audit; consideration will therefore be required to undertake further audit testing regarding the Council's compliance with data protection regulations in a future Audit Plan. Findings from the audit undertaken noted the following areas for consideration:-

- UK GDPR requires the Council to undertake regular monitoring of policy compliance to ensure data handling and security controls are operating effectively in practice. This is not being undertaken. Further monitoring arrangements should be introduced to evidence compliance with UK GDPR and the Council's Data Protection Policy.

- It was noted that the Council does not maintain an Information Asset Register or a formal Record of Processing Activities. A requirement of UK GDPR is a need to record data flows and document a register of personal data. This should also assist in facilitating a risk assessment of information areas where further controls may be required.

- It was pleasing to note that officers need to complete Council online training modules on data protection. However, no monitoring of participation has been undertaken. A review should be done to highlight officers that have not completed this training module. Any officer identified should be reminded to undertake their data protection training requirement.

Recommendations

Risk Ratings for Recommendations						
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	Medium	Less critically important controls absent, not being operated as designed or could be improved.		Low	Lower level controls absent, not being operated as designed or could be improved.
No.	**Audit Recommendation**	**Priority**	**Accepted (Yes/ No)**	**Comments**	**Responsible Officer**	**Timescale for Implementation**
Key Control: The Council has the appropriate procedures and controls in place to protect information, fulfilling the requirements of GDPR.						
5.01	The Data Protection Policy and guidance should be reviewed to ensure the detailed information remains current and appropriate. Thereafter, a timetable for continued review should be set.	Medium	Yes	Task already identified and awaiting workload capacity.	Records & Heritage Manager and Data Protection Officer	31/01/2023
5.02	In compliance with UK GDPR, a Record of Processing Activities (ROPA) should be compiled by the Authority based on a data mapping exercise.	High	Yes	A Data Protection Review is already underway with the Information Governance Officer post now in place. Information collected from the 2018 GDPR introduction work will form the basis of this review. A finalised ROPA and Information	Records & Heritage Manager and Data Protection Officer	31/12/2023

Risk Ratings for Recommendations						
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	Medium	Less critically important controls absent, not being operated as designed or could be improved.		Low	Lower level controls absent, not being operated as designed or could be improved.
No.	**Audit Recommendation**	**Priority**	**Accepted (Yes/ No)**	**Comments**	**Responsible Officer**	**Timescale for Implementation**
				Asset Register will be produced, and retentions, privacy notices and training all highlighted too.		
5.03	In compliance with UK GDPR, an Information Asset Register should also be compiled and maintained on an ongoing basis.	High	Yes		Records & Heritage Manager and Data Protection Officer	31/08/2023
5.04	A review of Privacy Notices held within Council services should be progressed and the documents made available on the Council website for public inspection.	Medium	Yes	Privacy notices (PNs) are covered in the current DP Review, as the current PNs are updated or new PNs created they are made available on the Council's website. After the review this will be an ongoing process whenever a change in the data process	Records & Heritage Manager and Data Protection Officer	31/08/2023

Risk Ratings for Recommendations						
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	Medium	Less critically important controls absent, not being operated as designed or could be improved.		Low	Lower level controls absent, not being operated as designed or could be improved.
No.	**Audit Recommendation**	**Priority**	**Accepted (Yes/ No)**	**Comments**	**Responsible Officer**	**Timescale for Implementation**
				occurs.		
5.05	Consideration should be given to undertaking reviews within Services to audit compliance with the Data Protection Policy and Guidance. This should provide assurance that the Authority is effectively handling personal data in line with regulations.	High	Yes	Current DP Review will assist this. Due to workload pressures, reviews will only be undertaken when investigating data breaches.	Records & Heritage Manager and Data Protection Officer	31/08/2023
5.06	A review of the guidance documents and forms held within the Information Management section of the Interchange should be undertaken and updated accordingly.	Low	Yes	When workload capacity allows, these guides are reviewed, updated and promoted.	Records & Heritage Manager and Data Protection Officer	30/09/2023
5.07	A review should be undertaken of the officers that have not undertaken the data protection training on the LearnPro training system. Any officer identified should be reminded to undertake their data protection training requirement.	High	Yes	Staff are reminded to do training via interchange news items and in response to data breaches. However, policing the completion of	Records & Heritage Manager and Data Protection Officer	30/04/2023

Risk Ratings for Recommendations						
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	Medium	Less critically important controls absent, not being operated as designed or could be improved.		Low	Lower level controls absent, not being operated as designed or could be improved.
No.	**Audit Recommendation**	**Priority**	**Accepted (Yes/ No)**	**Comments**	**Responsible Officer**	**Timescale for Implementation**
				mandatory modules could be given a higher priority.		
5.08	Consideration should be given to providing elected members with an update of actions undertaken to ensure the Council's compliance with data protection requirements.	High	Yes	Agreed this should become a regular annual report.	Records & Heritage Manager and Data Protection Officer	31/12/2023