INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	Information Governance – Council's Compliance with General Data Protection Regulations
TO:	Deputy Chief Executive (AJ)	**DATE:**	9 March 2018
C.C.	Chief Executive Head of Finance Democratic Services Manager Information Governance Manager Portfolio Holder (Cllr AM)		

---

1 Introduction

1.1 In accordance with the Audit Plan for 2017/18 a review of the forthcoming General Data Protection Regulations (GDPR) under the Audit Plan umbrella of Information Governance has been completed. This report presents the findings and conclusions drawn from the audit for information and action where appropriate.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and co-operation received during the audit.

2 Background

2.1 The purpose of the audit was to ensure that the Council is adequately prepared for the forthcoming changes to the General Data Protection Regulations. This change is due in May 2018.

2.2 The EU General Data Protection Regulations will affect every organisation that processes the personally identifiable information (PII) of EU residents. The introduction of the GDPR represents the most significant change to data protection law in the UK, EU, and globally, in recent years. Every organisation must be aware of the requirements of the GDPR as we are now in the transition phase leading up to May 2018.

2.3 Key to the new regulations will be an increase to the rights of data subjects who will have a greater influence on how their data is processed. Other significant areas of change include the rules on consent and the requirement for a dedicated data protection officer role. The Regulation also mandates considerably tougher penalties for data breaches than under the current law, from a theoretical maximum of £500,000 that the ICO could levy under current legislation (in practice, the ICO has never issued a penalty higher than £400,000), penalties under GDPR have an upper limit of €20 million

(approx. £17million) or 4% or annual global turnover, whichever is the higher.

2.4 At the time of the audit, the Council was in the process of appointing a Data Protection Officer (DPO). This post will be a shared role with Stratford on Avon Council. The recruitment process has meant that the process of addressing GDPR within the Council had been put on hold until the expertise that the new post will bring becomes available.

3 Scope and Objectives of the Audit

3.1 The audit was an assurance review of the information governance arrangement in light of the legislation changes in 2018. There was an advisory element to provide some guidance as to the likely impact on technical controls which the new Act imposes.

3.2 Because of the 'in limbo' status of this process, limited testing has been possible. Some work has commenced but has halted until the new DPO is in post and can analyse the prevailing arrangements and make the necessary changes. Such testing as was possible has been performed to confirm that controls identified have operated as expected with documentary evidence being obtained where possible, although some reliance has had to be placed on verbal discussions with relevant staff.

3.2 The audit scope included:

Information management (policies, ownership, asset categorisation).
Information-sharing arrangements.
ICT technical requirements, if clear and known.

4 Findings

4.1 Recommendations from Previous Report

4.1.1 This section is not relevant as this is the first audit of this area.

4.2 GDPR Management Arrangements

4.2.1 Essentially this involves the requirement for a dedicated Data protection Officer (DPO) role. At the time of the audit, this role did not exist but was being recruited. It is planned that a shared resource (with Stratford on Avon) will be appointed. In the meantime, the responsibilities were being covered by Graham Leach, the Council's Democratic Services Manager and Deputy Monitoring Officer. The Data Protection Officer role will be the key coordinator of the activities necessary to promote the awareness and lead the compliance preparation activities. Although this key control was not in place at the time of the audit, it was clearly being addressed therefore no recommendation has been made. However, the relatively late appointment and the planned (part-time) resource allocation might be insufficient in the short term to ensure that the Council has the necessary compliance arrangements in place by the May 2018 deadline.

4.2.2 There are aspects to GDPR management that would normally fall within the responsibility of a DPO. These include Policy and procedure development,

awareness raising, training. The former is dealt with elsewhere in this report, but the remaining two will need to have swift actions taken once the new DPO is in post.

Risk

Staff may lack awareness of the Council's and their own responsibilities.

Recommendation

A programme of targeted awareness raising events (workshops, short training courses/sessions, etc.) and updated communications for Council staff should be introduced at an early point once the new person is in post.

4.3 **Information Management**

4.3.1 We were informed during the audit that policies for IG had started to be drafted, but that this had been halted until the new DPO was in post.

4.3.2 There are a number of policies that may require amending to ensure GDPR compliance. Specific IG (GDPR) policies, also information security and any associated policies (e.g. HR).

Risk

Policy documentation may be out of date and the Council is non-compliant.

Recommendation

A full review of all relevant policies and procedures should take place once the new officer is in post.

4.3.3 There is a requirement to ensure that information accountability is in place. This is a recurring theme in GDPR. This is not new but rather than being implicit, as in the Data Protection Act, GDPR emphasises its significance. This would normally be achieved by the introduction of information assets owners. This had yet to be implemented at the time of the audit. The new accountability principle in Article 5(2) requires the Council to demonstrate compliance with the principles and states explicitly that this is the Council's responsibility. The Council is expected to put into place comprehensive but proportionate governance measures.

Risk

Non-compliance with legislation.

Recommendation

An information audit should be undertaken and Information Asset Owners should be appointed (and trained as appropriate) as soon as practical.

4.3.4 A key element of GDPR is "data protection by default" which requires mechanisms to be in place within the Council to ensure that, as a matter of routine, only personal data which are necessary for each specific purpose are processed. This obligation includes ensuring that only the minimum amount of personal data is collected and processed for a specific purpose; the extent of processing is limited to that necessary for each purpose; the data are stored no longer than necessary and access is restricted to that necessary for each purpose. As part of a "data protection by design" approach, a data protection impact assessment (DPIA) will become a mandatory pre-requisite before processing personal data which is likely to result in a high risk to the rights and freedoms of individuals. The Council should consider how it will implement DPIAs for relevant personal data processing systems (e.g. Council Tax, Housing Benefits).

Risk

Non-compliance with legislation.

Recommendation

The Council should document and implement a procedure for Data Protection Impact Assessments (DPIA).

4.3.5 To assist with meeting Article 30 the Council will need to look closely at its Information Asset Register (IAR) process and undertake an information audit across all services to map data (items and flows). Based on our discussions, it was not clear whether or how up-to-date the services' IARs are.

Risk

Non-compliance with legislation.

Recommendation

A comprehensive information audit should be undertaken to formulate an Information Asset Register sufficient to meet the requirements of Article 30.

4.4 Information Sharing

4.4.1 To help comply with the GDPRs accountability requirements the lawful basis of processing should be fully documented along with any sharing requirement/partners. Where sharing is carried out, the IAR should provide a link to the information sharing agreement signed by all parties to the sharing. Under the GDPR, some individuals' rights will be modified depending on the lawful basis for processing their personal data.

Risk

Non-compliance with legislation.

Recommendation

The Council should review and /or introduce compliant information sharing agreements.

4.4.2 Articles 44 to 50 introduce new rules for transfers of data to other countries or international organisations. We did not identify such transfers during our discussions, however particular attention should be applied to any existing or future cloud service facilities / systems used or hosted solutions to ensure the system owners are fully aware of where the processing of Council data is taking place. This should be considered either during the information audit process (recommendation 4 refers), as part of new system acquisitions or as a separate focussed exercise and the guidance provided by the ICO followed where necessary. Future considerations should be addressed through the PIA / DPIA process. This is provided for guidance only – not an action point at this time.

4.5 Technical Requirements

4.5.1 Detailed information about the detailed technical security implications of GDPR are limited at the time of drafting this report. In addition, the GDPR Articles talk of "*implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk*". Our research has revealed little at this stage that specifically states, or provides exemplar information on which to draw. Our research shows that GDPR Article 32 describes the security of processing standards and this is where relevant information might be found. Article 32 states that those appropriate measures as mentioned above should take into account the "*state of the art*" (taken to mean the technologies at the Council's disposal), "*the cost of implementation"* and "*the nature, scope context and purpose of the processing"* as well as "*the risk…"*.

4.5.2 Article 32 identifies the following as the kinds of security actions that might be suitable to the risk:

- Pseudonymisation of personal data;
- encryption of personal data;
- confidentiality, integrity and availability of personal data
- resilience of processing systems;
- ability to recover and restore access to personal data in a timely manner in the event of an incident; and
- the introduction of a process that regularly tests and evaluates the effectiveness of controls and processes for ensuring security of processing.

4.5.3 Because GDPR does not describe specific technical measures to be used to secure personal data, means that this is left open to interpretation. Commentators are suggesting that the current legislation has set broad goals whilst the detail will be forthcoming in future updates. It is known that GDPR takes a risk-based approach to data security and confidentiality. The higher the risk, the greater the need (and therefore likely greater cost/effort) of the required solution.

4.5.4 Our research has revealed that Article 32, which replaces Principal 7 as the relevant standard, has actually changed very little in terms of content. It is therefore apparent that good quality, robust controls will be a strong starting point for compliance with GDPR in technical terms. There are other, external standards or guidance that will help in this regard. The ISO standard for Information Security Management (ISO27k) is relevant, as is the PCI-DSS compliance standard. This along with the Cyber Essentials Scheme guidance will provide very useful baselines of control for GDPR compliance. Compliance with these industry standards will also greatly increase the likelihood of compliance with GDPR.

4.5.5 It should be remembered that the above is about the processing and protection of personal information for GDPR compliance.

4.5.6 The ICT Audits undertaken in previous years will also be a source of relevant information in order to ensure good baselines of control; the relevant ones were:

- Change Management (2016/17)
- Patch Management (2016/17)
- ITDR (2016/17)
- Total Finance – Application review (2016/17)
- Civica – Application reviews (2015/16)
- Data Security (2015/16)
- PSN (2015/16)
- Infrastructure (2014/15).

4.5.7 Other sources of authoritative guidance include the following:

- National Cyber Security Centre – 10 steps for monitoring to detect attacks.
- CIS Critical Security Controls for Effective Cyber Defence.

5 Conclusions

5.1 The audit identified three 'High' and three 'Medium' rated recommendations, giving, at this stage, a LIMITED level of assurance for the Council's compliance with the impending General Data Protection Regulations. It is recognised that the new Data Protection Officer post-holder should be in place now and some of the issues identified at the time of the audit may now have been, or are being, tackled and this will be reflected in the management responses to the findings.

5.2 The assurance bands are shown below:

Level of Assurance	Definition
Substantial Assurance	There is a sound system of control in place and compliance with the key controls.
Moderate Assurance	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited Assurance	The system of control is generally weak and there is non-compliance with controls that do exist.

6 **Management Action**

6.1 The recommendations arising above are reproduced in the attached Action Plan (Appendix A) for management attention.

Richard Barr
Audit and Risk Manager.

Appendix A

Action Plan

Internal Audit of the Council's Compliance with General Data Protection Regulations – March 2018

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.2.2	A programme of targeted awareness raising events (workshops, short training courses/sessions, etc.) and updated communications for Council staff should be introduced at an early point once the new person is in post.	Staff may lack awareness of the Council's and their own responsibilities.	Medium	Democratic Services Manager	An awareness briefing session is being designed for roll out via meta compliance to go out in in March.	Week Commencing 19 March 2018
4.3.2	A full review of all relevant policies and procedures should take place once the new officer is in post.	Policy documentation may be out of date and the Council is non-compliant.	High	Information Governance Manager	A report is being brought to Executive in April seeking approval of the Information Governance Framework and associated high level polices. This will also set up the framework for approval of relevant guidance.	5 April 2018

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.3.3	An information audit should be undertaken and Information Asset Owners should be appointed (and trained as appropriate) as soon as practical.	Non-compliance with legislation.	High	Information Governance Manager & Heads of Service	The Information Audit is underway with returns being received from Service Areas. Heads of Services are the Information Asset Owners this is being embedded in new Information Governance Policies. Training sessions are being provided as required along with a pre-briefing before the role out of each audit.	In place and ongoing
4.3.4	The Council should document and implement a procedure for Data Protection Impact Assessments (DPIA).	Non-compliance with legislation.	High	Information Governance Manager	This document is in draft form ready to go through the approval process	30 April 2018
4.3.5	A comprehensive information audit should be undertaken to formulate an Information Asset Register sufficient to meet the requirements of Article 30.	Non-compliance with legislation.	Medium	Information Governance Manager & Heads of Service	The Information Audit is underway with returns being received from Service Areas. (20 out of 24 teams have started, four are nearly completed) Progress is being monitored and teams are being actively supported with the audit.	6 April 2018

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.4.1	The Council should review and / or introduce compliant information sharing agreements.	Non-compliance with legislation.	Medium	Information Governance Manager	Information sharing with partner agencies is being identified through the information audit, and via a review of third party and contract arrangements. There will be an action plan for each agreement where non-compliance is identified.	May 2018

* Risk Ratings are defined as follows:

High Risk: Issue of significant importance requiring urgent attention.
Medium Risk: Issue of moderate importance requiring prompt attention.
Low Risk: Issue of minor importance requiring attention.