TONBRIDGE & MALLING BOROUGH COUNCIL

AUDIT COMMITTEE

25 July 2022

Report of the Director of Central Services & Deputy Chief Executive

Part 1- Public

Matters for Information

1 INTERNAL AUDIT AND COUNTER-FRAUD UPDATE – GDPR STORAGE LIMITATION

1.1 Introduction

1.1.1 At the previous meeting of this Committee on 4 April 2022, Members were provided with an update on the work of both the Internal Audit function and the Counter Fraud function for the period April 2021 to March 2022.

1.1.2 Members' attention was drawn to the issue of a 'No Assurance' opinion in respect of the audit findings on Data retention, principle 5 of the General Data Protection Regulation (GDPR), as set out in Annex 1 to the report. Members expressed serious concern about this opinion and requested that the Data Protection Officer and the Chief Audit Executive provide an update report on this matter to the next meeting of the Committee.

1.1.3 This report updates Members on progress in complying with the recommendations in the Audit report.

1.2 Update

1.2.1 The internal audit report dated 13 January 2022 made 5 recommendations. These are set out below together with the actions taken by way of response.

1.2.2 **Recommendation 1** – Split responsibilities for the Data Protection Officer (DPO) & Senior Information Risk Owner (SIRO) between different officers and update the Information Governance Policy to reflect the change in responsibilities.

1.2.3 The roles of DPO and SIRO no longer sit with the same Officer. The role of DPO (which is a statutory role) remains with the Director of Central Services, with discussions taking place with another Officer for the role of SIRO (a non-statutory role) to be re-assigned to them. In the interim, all service managers (as Information Asset Owners) are responsible for management of the risks associated with the information processed by their respective services.

1.2.4 Any staffing implications associated with the re-alignment of responsibilities will be reported to the General Purposes Committee.

1.2.5 The Information Governance Policy has been updated to reflect the removal of the responsibility for the SIRO role from the Director of Central Services. The Policy will be further updated upon re-assignment of the SIRO role.

1.2.6 **Recommendation 2** – The Head of Licensing and Community Safety should put a Data Retention schedule in place for both Licensing and Community Safety as soon as practical.

1.2.7 This was completed in December 2021, prior to the publication of the final audit report.

1.2.8 **Recommendation 3** – Ensure that all retention schedules are subject to regular and documented reviews.

1.2.9 In response to this recommendation, all service were requested to review their retention schedules. At the time of preparing this report, only 1 review (out of a total of 32) was outstanding and this has been chased with the service in question. In future all retention schedules will be subject to annual review.

1.2.10 **Recommendation 4** – Ensure that all services are delete electronic data held on software systems in accordance with the retention schedule for the service.

1.2.11 The Council holds data on a number of different software systems, with the principal system being Uniform (supplied by IDOX), an electronic document and records management system used by many frontline services including Planning, Building Control, Land Charges, Environmental Health, Environmental Protection, Housing, Licensing, Anti-social Behaviour, Estates, Gazetteer and Street Naming and Numbering services.

1.2.12 The Council has previously purchased a data disposal module for Uniform. However, the implementation of this module raised concerns amongst staff, as it presented a risk of inadvertently deleting inter-dependent data that we needed to retain. The implementation of the module would the implementation of this would be time-consuming and incur additional consultancy costs from IDOX. Given these specific risks the module is not currently operational.

1.2.13 Members will be aware that the Council is in the process of migrating from Uniform to a new document/ records management system (Agile), as reported to Cabinet on 15 March 2022. Written notice has been given to IDOX, the supplier of the Uniform system, that the Council will not commit to this system beyond 31 March 2023. The new Agile system will therefore be implemented by this date.

1.2.14 The new Agile service will be compliant with GDPR requirements (including deletion of data at the end of any retention period) as part of the service design via scripts. These pre-built scripts will be developed and agreed prior to implementation of Agile. This will then remove the necessity for manual deletion of data records at the end of any given retention period.

1.2.15 Of the internally hosted systems/ platforms, the current position is as follows:-

- Intergra – We are required to keep data for the current financial year plus 6 years on the system. The system is purged of data prior to this as part of the year end processes, this will include unused suppliers and customers on our Purchase and Sales (respectively) Ledgers.

- We use Ebase as a platform to develop specific workflow processes across the Council e.g. complaints. The deletion of data from these is being progressed by IT in consultation with the relevant services.

1.2.16 A number of other systems/ platforms used by the Council are externally hosted e.g. JADU/ CXM, Locata, Whitespace, A365. Responsibility for data deletion from those systems rests with the external host.

1.2.17 Work is underway by IT Services to ensure that all emails are deleted automatically from Netguard (our email archive system) after 12 years. This is the long-stop date within our adopted data retention policy.

1.2.18 **Recommendation 5** - Ensure that once Retention Schedules have been reviewed and updated, privacy notices are also reviewed and updated so that both are aligned.

1.2.19 All privacy notices have been reviewed since the date of the audit to ensure that they are current and align with the relevant service privacy notice. These will be subject to annual review.

1.2.20 All privacy notices are available to view on the Council's website at TMBC privacy notices by service – Tonbridge and Malling Borough Council.

1.3 Legal Implications

1.3.1 The UK General Data Protection Regulation contains 6 principles which the Council (as a Data Controller) must comply with. This includes the principle of storage limitation i.e., we are required to ensure that the period for which personal data is stored is limited to a strict minimum and establish time limits for erasure or for a periodic review in order to ensure that personal data is not kept for longer than necessary.

1.3.2 As a public authority the Council is required to appoint a Data Protection Officer in compliance with Article 37 of the GDPR.

1.4 Financial and Value for Money Considerations

1.4.1 None arising from this report.

1.5 Risk Assessment

1.5.1 The Council has statutory obligations under the UK GDPR and the Data Protection Act 2018. Failure to meet those obligations may result in enforcement by the Information Commissioner, including the imposition of fines.

Background papers: contact: Adrian Stanfield

Nil