Committee(s)	Dated:
Digital Services subcommittee	26 September 2019
Subject: General Data Protection Regulation (GDPR/Data Protection Act 2018 (DPA))	**Public**
Report of: Michael Cogher, Comptroller & City Solicitor	**For Information/Decision**
Report author: Sophie Jordan, Information Compliance Manager	

Summary

This report provides a general update on the final phase of the work to embed GDPR/DPA implementation into the Corporation. A further external audit commenced in July 2019 it is anticipated that this audit will conclude in September 2019 and will be reported to committee when finalised.

Recommendations

Members are asked to note the report.

Main Report

Introduction

1. This Report outlines the status of actions arising from phase 2 of the GDPR project including the steps taken to address the recommendations of the internal audit by Mazars previously reported to Committee.

GDPR Project progress

2. Phase 2 of the GDPR implementation project was closed on 28th March 2019 on the basis that GDPR was largely embedded as business as usual across all departments.

3. Two key priorities were identified in the May 2018 Mazars GDPR compliance audit these were reviewing third party contracts for GDPR compliance/data processing agreements and a full review and revisions of the Corporation records retention policy. In relation to third party contractors/data processors all contracts were reviewed in some cases contracts have been terminated or no longer used. The remaining existing contracts are GDPR compliant or are in the processing of becoming so. Contractor data processing arrangements will continue to be audited using the compliance monitor. The perceived lack of a record retention schedule was rated as a high priority in the Mazar's audit. Good progress has been made by departments in putting revised retention schedules in place and in reissuing of the overarching schedule, this work is now largely complete with a few departments currently updating departmental schedules.

4. A further GDPR compliance audit is being undertaken by Mazars which commenced in July 2019 and which it is anticipated will be concluded in September 2019 the focus of this audit is on staff training; the compliance and monitoring of Data Protection/GDPR practices by use of the self-audit monitor; compliance with the fourth principle of the DPA 2018 that personal data should not be kept for longer than is necessary; compliance with the sixth data protection principle, that all information should be kept secure; the implementation of retention schedules, data breaches and compliance with other data subject rights, i.e. the right of erasure.

5. Departments were issued with a self-audit template in November 2018 with a second tranche in February 2019 which covered the key activities, processes and arrangements that are required to ensure GDPR/DPA compliance, all departmental audits have now been completed.

6. Completion of the core tasks required of departments to achieve full GDPR compliance is currently
   - 68% full implemented
   - 19% are partially implemented
   - 0% are not yet started
   - 13% of the core tasks do not apply to the department in scope.

   The GDPR compliance monitor summary is attached as Appendix 1.

7. IT Services are covered by two separate monitors, one which covers the GDPR specific compliance tasks and a second for Systems and Data Security of which 87% of the core tasks monitored are fully implemented.

Information governance

8. Information governance was rated as low risk by the Mazar's audit report.

9. The C&CS Information Compliance Team continue to provide advice and support to departments on all issues relating to GDPR compliance and liaises with the Data Protection Officer on issues in relation to GDPR.

10. GDPR Corporate Risk CR 25 was created, agreed by Audit & Risk Committee and continues to be actively managed, monitored and reported to both the Corporate Risk Management Group and to committee.

11. Regular liaison with IT workstreams is taking place which are reported to the GDPR Project Team for action and to the Information Management Board.

Training and communication

12. A mandatory GDPR e-learning training package was launched in April 2018, compliance levels are monitored by the Data Protection Officer and reported to Chief Officers. The current training compliance level of staff who have undertaken the training or are exempt is 94.18% as of the 19 August 2019.

13. An Access to Information Network representatives (AIN) forum was established in 2018 and meets quarterly to discuss and raise topical GDPR issues and initiatives. A Microsoft Teams GDPR page is in place for knowledge sharing.

Data Breaches

6. Under GDPR there is a duty to notify the ICO of data breaches posing a risk to individuals' rights without undue delay, and where feasible within 72 hours of becoming aware of the breach. Where there is a high risk to data subjects they must also be informed. The Corporation has suitable arrangements in place for dealing with data breaches. Between 1 January 2019 to 22 August 2019 there have been 45 breaches notified to the Data Protection Officer. Of those 45, 2 were judged to be notifiable to the ICO. The ICO has responded to 1 indicating that no further action needed to be taken but made recommendations which were implemented, and the remaining notifiable breach is currently awaiting a response from the ICO.

14. Of the 2 reported to the ICO, one related to the disclosure of the address of a young person in care, via documentation provided to the young person's parents who were not allowed to have access to that data. In this instance the young person was made aware of the incident and was sent a formal apology letter. The second incident relates to a secure bag containing a variety of documents in relation to a small number of data subjects, being stolen. We note that the documents included both personal and special category data. In this instance 2 of the individuals concerned have been notified and a risk assessment is currently being undertaken as to whether to inform the remaining individuals.

Conclusion

15. GDPR places significant obligations on the Corporation in relation to the processing of personal data to protect the rights and freedoms of everyone.

16. The GDPR Project Team consider that the Corporation has largely achieved material compliance with GDPR/DPA requirements with GDPR now regarded by departments as business as usual.

17. A final Mazar's audit in relation to data Protection and GDPR is being undertaken currently and the outcome will be reported to Committee in due course.

Appendices

1. GDPR Compliance Monitor – Summary – July 2019

Michael Cogher
Comptroller & City Solicitor,
Tel: 0207 332 3699,
Email: michael.cogher@cityoflondon.gov.uk