Committee(s)	Dated:
Information Technology Sub-committee Audit and Risk Management Committee	02/11/2018 06/11/2018
Subject: General Data Protection Regulation (GDPR) Audit	**Public**
Report of: Michael Cogher, Comptroller & City Solicitor	**For Information**
Report author: Michael Cogher, Comptroller & City Solicitor,	

Summary

This report presents the outcome of the internal audit of phase 1 of the Corporation's arrangements for compliance with the General Data Protection Regulation (GDPR) which came into force on 25th May 2018 together with a general update on the phase 2 activities. Oversight of GDPR is the responsibility of the IT Sub-committee and the Audit and Risk Management Committee.

Recommendations

1. Members are asked to note the report.

2. To determine the frequency of further GDPR monitoring reports and in particular in relation to data breaches.

Introduction

1. The EU introduced updated and harmonised data protection regulations known as the General Data Protection Regulation (GDPR) which came into force on 25 May 2018.

2. This Report outlines the steps that the Corporation has taken to ensure that it is GDPR compliant, the findings and recommendations of the internal auditors, Mazars, and the work being undertaken in phase 2 of the GDPR project which commenced on 25th May 2018.

GDPR Project Progress

3. The first phase of the Corporation's preparations for GDPR were completed in advance of the GDPR implementation date of 25th May 2018. In summary these included a review and revision of the Corporation's information governance practices, policies and procedures, privacy notices; training and awareness raising; and ensuring the necessary technical IT and information security systems are GDPR compliant.

4. These tasks were the subject of phase of a detailed project plan overseen by the Information Board and IS Steering Group and delivered by the GDPR Project Team and departmental Access to Information Network Representatives (AIN) and management teams. Member scrutiny and member level decision making was undertaken by the IT Sub-Committee and the Policy and Resources Committee.

5. The Comptroller & City Solicitor was formally appointed by committee as the Corporation's Data Protection Officer (DPO) in November 2017. The role of the DPO is to inform and advise the organization as to its obligations under GDPR, monitor compliance, advise on data protection impact assessments and co-operate and act as a contact point with the ICO. Chief Officers remain responsible for the use and security of personal data held by their departments and institutions.

6. The GDPR implementation project plan covering all tasks required to effectively prepare for GDPR compliance was created in September 2017 and audited by Mazars with a positive outcome and with no minor or major risks to project delivery identified. A further audit was undertaken by Mazars in late May 2018 to assess the Corporation's readiness and levels of compliance with GDPR requirements. The Mazars audit adjudged the Corporation to be 'materially compliant with GDPR requirements', the GDPR Project Team found the findings of the Mazar's report to be broadly accurate, some of the recommendations had already been incorporated into the GDPR phase 2 project plan. The GDPR Project Team responded to Mazar's report and a final draft was received from Mazar's in October 2018 (Appendix 1) with a reduced number of high priorities based on feedback from the GDPR Project Team. The auditor's recommendation and the management response are set out in Appendix 1, pages 7 to 14 of the report.

7. Phase two GDPR project which runs from 25 May 2018 to 31 December 2018 aims to further embed and refine GDPR knowledge and compliance across the Corporation with the following priority areas:

    - Reviewing third party contracts for GDPR compliance (considered high priority by Mazars).
    - Reviewing and refining the overarching Corporation records retention policy and developing detailed departmental records retention policies (considered high priority by Mazars).
    - Auditing departmental compliance with GDPR requirements, advising and further embedding GDPR compliance as business as usual (considered low priority by Mazar's but viewed as critical to GDPR compliance by the GDPR Project Team).

GDPR Departmental Self-audit Monitor

8. Mazar's identified 'that there is a risk that implementation of tasks may not be sufficiently monitored in departments'.

9. To further embed GDPR as standard operational practice in departments a GDPR Self-Audit Monitor has been developed covering the key elements required for GDPR compliance (Appendix 2) for the departments which process large volumes of personal data and this was issued for completion by AIN representatives in Departments with a deadline of 31 October 2018.
   Once completed and returned the C&CS Information Team will undertake audits and advise AIN representatives on risk areas that require rectification and on how greater levels of compliance can be achieved. Progress and identified high risk areas will be reported to the Data Protection Officer, and where required IT Sub-committee and the Audit and Risk Management Committee.

10. Detailed guidance tailored to departments is on-going and will continue as department specific GDPR issues and risks arise particularly from the departmental compliance audits.

Third Party Contractors

11. This is an area rated as high priority by the Mazar's audit. The standard data protection clause was revised and has now been incorporated in all new contracts. All existing contractors received a written request for a response to confirm that they are GDPR compliant. 20 departments have been asked to complete a Contracts Register for live contracts with third parties who process personal data on behalf of the City of London Corporation, as a data controller. This register is used to identify key requirements of the GDPR for 3rd parties - if sub-processors are used, if procurement data protection schedules are in place and whether a Data Protection Impact Assessment is required. Of the 20 departments, 8 (40%) have completed the register, 5 (35%) confirmed they do not have such contracts and 7 (25%) departments are still working on the register.

12. A deadline of 31st October 2018 was issued to departments for the completion of and return of this register. The GDPR team will review the returns and determine any further action required (Appendix 3).

Records retention policy and schedules

13. The perceived lack of a record retention schedule was rated as a high priority in the Mazar's audit. The position across the Corporation remains mixed, with some areas of good practice and others needing improvement. The existing model records retention policy and schedule originally devised by the LMA was reviewed, revised and re-issued on the intranet. Departments were requested to complete a more detailed records retention schedule and 64% have done so thus far. Further, 14% of record retention schedules are currently work in progress and 22% of departments have not yet submitted a schedule (Appendix 3).

Information governance

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

15. GDPR Corporate Risk CR 25 was created, agreed by Audit & Risk Committee and continues to be actively management, monitored and reported to both the Corporate Rik Management Group and to committee. The CR 25 Risk report is attached as (Appendix 5).

16. Project delivery is controlled at bi-weekly Project Team stage control meetings which monitor progress, capture GDPR issues and risks, assess required changes and associated corrective action and allocate work packages. The Project Team reports to the Information Board and IS Steering Group, additionally update reports and revised policies are reported to Policy & Resources and Establishment Committees and to IT sub-committee.

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

Training and communication

18. Six half day training sessions for AIN representatives and key staff were by the Comptroller & City Solicitor and Senior Information Compliance Officer all AIN representatives have undertaken the initial training. Further focused training has been provided to the HR Department, Remembrancer's Events Team, EDO. Quarterly AIN representatives' training and networking events have commenced with the first session taking place on 5th October 2018.

19. Five training sessions for Members were delivered, and member guidance substantially revised to incorporate GDPR requirements, template forms issued including RoPA, Privacy notices.

20. A mandatory GDPR e-leaning training package was launched on City Learning on 23 April 2018 compliance levels were monitored by the Data Protection Officer and reported to Chief Officers current take up is over 94% (Appendix 4).

21. The GDPR corporate communications plan was agreed with the Communications Team and launched on 8 May 2018, further communications drives will be scheduled.

22. An initial GDPR intranet page has been updated to include guidance, news, policies, procedures, the relevant forms and FAQ's. This will further be updated in due course.

Data Privacy Impact Assessments

23. A data Privacy Impact Assessment template was developed and tested on the corporate CRM project and has now been refined, adopted and incorporated into the corporate project management toolkit and Corporate procurement process.

Policies

24. GDPR related policies have been revised to incorporate GDPR requirements including Employee Data Protection Policy, Data Protection Policy, Data Subject Rights Policy, Pupil and Parent Data Protection Policy, Data Breach Policy, Appropriate use of IT Policy, Information Security Policy, Storage of Data Policy, System Vulnerability Scanning Policy, Security Patching Policy and Procedure.

25. All staff will be required to re-read the key policies to refresh their knowledge and a MetaCompliance tracking tool will be used to monitor this.

Information Technology Systems

26. Requests for Tender have been sent to 4 potential providers of a software discovery tool which would be used to identify where personal data is stored at risk across the entire IT estate. Costs are required to assess the level of funding required.

Data Breaches

27. Under GDPR there is a duty to notify the ICO of data breaches posing a risk to individuals rights within 72 hours (where feasible) of becoming aware of the breach. Where there is a high risk to data subjects they must also be informed.

28. Since 25th May there have been 23 breaches notified to the DPO. A number of these related to pre-GDPR breaches. 5 were judged to be notifiable to the ICO. The ICO has responded to 3 indicating no action will be taken.

29. Of the 5, two related to mechanical problems with payslips/P60s, one to a misdirected email, one to a phishing attack and one to insecure use of post. In all cases Departments have been advised of appropriate steps to be taken to prevent future occurrences. Data subjects were notified in 4 cases.

30. The breach notification policy has been revised to provide that the Town Clerk, relevant Chief Officer(s), the Chairman of the IT Sub-committee and the relevant service committee Chairmen are notified of breaches notified to the ICO.

31. Members may wish to receive separate and more detailed reports, for example on a six-monthly basis, on data breaches.

Conclusion

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

33. The GDPR project has made significant progress, baseline compliance with GDPR requirements was achieved in May 2018 further work undertaken has reinforced and enforced compliance with GDPR requirements across departments. A further external audit during 2019 to measure levels of compliance across the Corporation will be considered in due course.

Appendices

1. Mazars Audit Report with management responses
2. Self-Audit Monitor Template and 2a. Guidance
3. Summary of competed Records Retention Schedules and Third-Party Contracts
4. Table: Departments completion of the Data Protection E-Learning Programme, as of 3 October 2018.
5. Pentana Report Risk

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