| Committee(s) | Dated: |
|---|---|
| Digital Services subcommittee<br>Audit and Risk Management Committee | 4th February 2019<br>12th March 2019 |
| **Subject:**<br>General Data Protection Regulation (GDPR/Data Protection Act 2018 (DPA)) | **Public** |
| **Report of:**<br>Michael Cogher, Comptroller & City Solicitor | **For Information/Decision** |
| **Report author:**<br>Michael Cogher, Comptroller & City Solicitor, | |


## Summary

This report provides a general update on the progress of phase 2 of the GDPR/DPA Implementation Project and the planned outcomes for the final phase of the work to embed GDPR/DPA implementation into the Corporation.


## Recommendations

1. Members are asked to note the report.

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

## Introduction

1. This Report outlines the status of phase 2 of the GDPR/DPA project. Including the steps taken to address the recommendations of the internal audit by Mazars previously reported to Committee.

## GDPR Project Progress

2. Phase two of the GDPR project commenced on 25 May 2018 and has been extended to 31 March 2019. This is to further assist departments to embed GDPR compliance with the following priorities identified in the May 2018 Mazar's GDPR compliance audit:

   - Reviewing third party contracts for GDPR compliance/data processing agreements.
   - Reviewing and refining the overarching Corporation records retention policy and developing detailed departmental records retention policies.

   The GDPR Project Team identified the following additional priority:

   - Auditing departmental compliance with GDPR requirements via a Compliance Monitor system, advising and further embedding GDPR compliance as business as usual.

**GDPR Departmental Compliance Monitor**

3. All Departments were issued with a self-audit template in November 2018 which covers the key activities, processes and arrangements that are required to ensure GDPR/DPA compliance. All departmental audits have been completed by the departments which process high-volume potentially high-risk personal data, these are:

   Markets and Consumer Protection
   DBE
   City Surveyors
   CoL School – Boys / CoL School – Girls / Freemens School
   DCCS and Community Safety
   Open Spaces
   Human Resources
   Remembrancers
   Chamberlains

   The following departments/teams are due to complete the self-audit by the end of February 2019:

   Electoral Services
   Comptroller & City Solicitor
   Mansion House
   Central Criminal Court
   Contact Centre
   Culture and Libraries
   Economic Development
   Occupational Health
   Guildhall School of Music & Drama

4. The GDPR team undertook a full analysis and audit of the completed returns and produced a compliance monitor; in terms of the core tasks which need to be completed to achieve full compliance, 51 % are fully implemented, 32% are partially implemented, only 2 % are not yet started and 15% do not apply to the department in scope. For example, processing of children's data and use of electronic communications used for marketing are not applicable to most departments. The current Self-Audit Monitors are updated every two months with the next return due at the end of February. A RAG summary of the departmental compliance self-audits is attached at Appendix 1. An example of a compliance self-audit is attached as Appendix 2.

5. Work is being undertaken with the responsible officers in each department (Access to Information Representatives (AIN)) and line managers to move partially implemented actions to fully implemented status during February. This is to ensure that work commences on the 2% of activities not yet started.

6. IT Services are covered by two separate monitors, one which covers the GDPR specific compliance tasks and a second for Systems and Data Security.

**Third Party Contractors/Data Processors**

7. This is an area rated as high priority by the Mazar's audit. The standard data protection provisions for Contractors/Data Processors was revised and has now been incorporated into all new contracts. All existing Contractors/Data Processors were issued with a written request to confirm that they are GDPR compliant and agreements have been amended where appropriate, of the 29 contracts which were outstanding in November 2018, all have reviewed, and appropriate amendments made. In some cases, contracts have been terminated or no longer used. This work is completed but data processing arrangements will continue to be audited using the compliance monitor.

**Records retention policy and schedules.**

8. 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, it is acknowledged that some departments have more complex records than others.

9. All but three departments have data retention schedules in place. City of London Girls School, Markets and Consumer Protection and Open Spaces are currently finalising their data retention schedules.

**Information governance**

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

11. 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.

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

13. 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**

14. Six half day training sessions for AIN representatives and key staff were given by the Comptroller & City Solicitor and Senior Information Compliance Officer. In 2018 all AIN representatives have undertaken the initial training.

15. Further focused training has been provided to the HR Department, Remembrancer's Events Team and EDO. Quarterly AIN representatives' training and networking events have commenced with the second session taking place on 24th January 2019.

16. Five training sessions for Members were delivered in 2018, and a Member's guidance booklet was substantially revised to incorporate GDPR requirements. Template forms were also issued including RoPA and Privacy notices.

17. 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. The current take-up is over 94.04%, as of the 1st January 2019. Full details are provided in Appendix 3. Due to staff turnover 94% constitutes a high level of compliance but the position will be kept under review. The ICO's expectation is that staff should have received training within the last two years.

**Data Breaches**

18. Under GDPR there is a duty to notify the ICO of data breaches posing a risk to individuals' rights within 72 hours (were feasible) 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. Since 25th May (to the 22 Jan 2019) there have been 48 breaches notified to the Data Protection Officer. Of those 48, 7 were judged to be notifiable to the ICO. The ICO has responded to 6 indicating no action will be taken.

19. Of the 7, two related to mechanical problems with payslips/P60s, one to an email held on an outlook folder which was visible to third parties, one to a phishing attack, one to third party data sent to the incorrect applicant as part of the recruitment process and two due 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 6 cases. Additionally, of the 7 reported to the ICO, 2 were in relation to activities undertaken by a processor on behalf of the Corporation.

20. The breach notification policy has been revised to provide that the Town Clerk, relevant Chief Officer(s), the Chairman of the Digital Services Committee and the relevant service committee Chairmen are notified of breaches notified to the ICO.

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

**Conclusion**

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

22. The GDPR project has made significant progress after achieving material compliance with GDPR requirements in May 2018. We are on target to meet the date of 31st March 2019 to close the project and move to business as usual. It is anticipated that a final compliance audit will be undertaken by Mazars following project closure. The Information Compliance Team will continue to monitor and audit departmental compliance with GDPR/DPA, but ownership and management of compliance will rest with departments with advice, training, support and monitoring provided by the Data Protection Officer.

**Appendices**

1. GDPR Compliance Monitor RAG Summary
2. Sample Departmental GDPR self-audit template
3. GDPR e-learning take up

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