Committee(s)	Dated:
Digital Services Sub (Finance) Committee	20 March 2020
Subject: General Data Protection Regulation (GDPR/Data Protection Act 2018 (DPA))	**Public**
Report of: Michael Cogher, Comptroller & City Solicitor	**For Information**
Report author: Sophie Jordan, Information Compliance Manager	

Summary

This report provides a general update on the final phase of the work undertaken to embed GDPR/DPA implementation in the Corporation and on the recommendations of a corporate GDPR compliance review audit undertaken in July 2019 and finalised in December 2019 (Appendix1).

Recommendations

1. Members are asked to note the report.

Introduction

1. Following the completion of the GDPR project in March 2019, this report details the status of key actions to be taken to address the recommendations of the internal audit undertaken by Mazars in July 2019 the aim of which was to verify that adequate arrangements are in place to ensure that the Corporation meets its GDPR obligations.

GDPR 2019 audit key findings and action to be taken.

2. Staff Training was identified as a key element in achieving GDPR compliance, all Corporation staff are required to complete GDPR e-learning module to ensure that they are aware of their responsibilities in relation to GDPR. The e-learning module was launched on 23 April 2018 prior to the GDPR implementation date. Some departments have staff who do not have access to the e-learning facility or had limited interaction with personal data and have been provided with alternative GDPR training.

   The C&CS Compliance Team produces a quarterly summary report which identifies the number of staff in each department who have completed the GDPR training or in progress, have not yet started the training or who are exempt.

   Audit testing identified members of staff who had not completed GDPR training despite two reminders to do so creating a risk that staff may not comply with data protection requirements. The Mazars audit recommendation was to sanction members of staff who have not completed the GDPR training after two reminders by revocation of network access, in practice this would be a time consuming exercise requiring an additional review of reporting mechanisms and would in fact

City of London Corporation - Official. This information remains the property of the City of London Corporation. Any requests to share this information in a public forum should be made through the City of London's Communication team.

create a risk as the reports generated from learning pool have been found to be inaccurate.

The current system of providing statistics on non-completion of GDPR training to Chief Officers and Access to Information representatives (AIN's) is a more effective solution and has contributed to a high level of compliance with GDPR training of 93.84% (completed, exempt or temporary exempt), as of the 25 February 2020 which given the level of staff turnover particularly temporary staff is still as high a level of compliance as can be reasonably expected if slightly lower than the 94% reported previously.

3. The audit identified a risk in relation to personal data held on corporate 'W' drives which currently contains 3500 folders some of which contain personal data which is likely to be sensitive and relates to ex-employees. 'W' drives were created to facilitate file transfers between departments and were not intended to be permanent repositories for data. Obsolete data held on 'W' drives creates a risk of data security breaches and a failure to comply with data protection requirements. Some attempts have been made to cleanse the 'W' drives of personal data but this is problematic as files are not grouped by departments. The audit recommended that data held on the 'W' drive should be reviewed and either deleted or transferred to a secure location.

   Market discovery work was undertaken by the IS division in 2018 to identify a suitable information discovery tool which would identify personal data held on the 'W' Drive however this was expensive the cheapest option being £80k and funding was not available in year to fund this. The Information Management Board agreed on 29th October 2019 to accelerate action to mitigate the 'W' drive risk, a plan will be developed to remove the 'W' drive and moving content to be retained with a timeline of five months from approval by the relevant officer groups and member committees the target for commencement is March 2020.

4. The maintenance of record retention schedules and the timely management of records disposal was rated as a high priority in the Mazar's audit. Significant progress has been made by departments in putting revised retention schedules in place and in reissuing the overarching schedule, this work is now largely complete with just two departments continuing to make progress to complete a comprehensive retention schedule. Both departments concerned have confirmed that some teams have localised retention schedules or have applied the overarching City of London retention schedule while the comprehensive version is being collated. The C&CS Compliance Team will continue to support departments in updating and maintaining retention schedules, furthermore retention schedules are monitored as part of GDPR self-audit monitors undertaken by departments on a quarterly basis, the target date for completion of all records retention schedules across the Corporation is 31 December 2020.

5. The Mazars audit tested the corporation's Data Protection Policy statement that 'data is only kept for as long as necessary in accordance with the retention schedules'. The audit established that implementation of records disposal dates is currently at various stages and that departments have not been running checks that obsolete data is being deleted in compliance with the records retention

City of London Corporation - Official. This information remains the property of the City of London Corporation. Any requests to share this information in a public forum should be made through the City of London's Communication team.

schedules resulting in the risk that obsolete personal data will be retained thereby failing to comply with the requirements of the Data Protection Act 2018.

The audit recommended that departments should be required to run regular audit checks on data and record deletion and that the C&CS Compliance Team should be notified of the results of the checks. The C&CS Compliance Team ceased undertaking compliance checks in late 2017/early 2018 due to the implementation of GDPR and a shortage of resource but in 2020 will be implementing new more thorough departmental compliance checks incorporating all aspects of the Data Protection Act 2018 including the implementation of records retention and deletion; the compliance checks will be monitored and departments advised of any required remedial actions.

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 31 December 2019 there were 68 breaches notified to the Data Protection Officer, with 3 judged to be notifiable to the ICO. For the period 1 January 2020 to 25 February 2020 there have been 12 breaches notified to the Data Protection Officer, with 1 judged to be notifiable to the ICO.

7. Of the 4 data breaches reported to the ICO during the period 1 January 2019 – 12 February 2020, 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, the documents included both personal and special category data. In this instance 2 of the individuals concerned have been notified and a risk assessment was undertaken as to whether to inform the remaining individuals, and it was decided to not notify them at the time of the incident, due to external factors. The third incident relates to the disclosure of personal data contained within a court bundle as a result of the use of incorrect redaction tools being used to redact personal data. The individuals concerned were informed of the incident and sent a formal apology. The final incident relates to the inappropriate disclosure of third party personal and special category data, predominately in relation to school pupils, as part of a panel hearing for a complaint raised against the school. This incident contained the personal and, in some instances, special category data in connection with approximately 147 data subjects. All data subjects have since been informed of the incident and sent a formal apology letter.

City of London Corporation - Official. This information remains the property of the City of London Corporation. Any requests to share this information in a public forum should be made through the City of London's Communication team.

Conclusion

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

9. 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.

10. It is anticipated that the further recommendations of the July 2019 Mazar's GDPR audit will be implemented and complied with by 31 December 2020.

Appendices

1. Mazars GDPR Audit July 2019
2. GDPR Compliance Review Audit Quarter 4 (October -December 2019)

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

City of London Corporation - Official. This information remains the property of the City of London Corporation. Any requests to share this information in a public forum should be made through the City of London's Communication team.