CITY OF LONDON

CHAMBERLAIN'S DEPARTMENT

INTERNAL AUDIT SECTION

CORPORATE WIDE

GDPR COMPLIANCE REVIEW

FINAL REPORT

Date Issued: December 2019

Issued to: Michael Cogher, Comptroller and City Solicitor
Sophie Jordan, Compliance Manager (Data Protection & Freedom of Information)
Nick Senior, Business Manager
Sean Green, IT Director

CONTENTS (INDEX)

Audit Fieldwork completed	September 2019
Draft Report Issued	October 2019
Management Response Received Agreeing Recommendations	November 2019
Final Report Issued	December 2019

SECTION A: EXECUTIVE SUMMARY

Introduction

1. This audit has been undertaken as part of the 2019/20 Internal Audit Plan.
2. The General Data Protection Regulation (GDPR), came into effect on 25 May 2018. The legislation is intended to strengthen data protection rights for individuals within the European Union.
3. Article 5 of the GDPR requires that personal data shall be:
    - Processed lawfully, fairly and in a transparent manner in relation to individuals;
    - Collected and used for specified, explicit and legitimate purposes;
    - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
    - Accurate and, where necessary, kept up to date (including taking every reasonable step to ensure inaccuracies are erased or rectified);
    - Kept in a form which permits identification of data subjects for no longer than necessary (for the purposes of which the personal data is being processed). This includes not storing information for longer than necessary, and
    - Processed in a manner that ensures appropriate security over the personal data.
4. Chief Officers at the City of London (CoL) have responsibility for compliance with the GDPR requirements. The Comptroller and City Solicitor is the CoL's Data Protection Officer, and is responsible for advising the CoL in relation to its obligations, monitoring compliance and training and liaising with the Information Commissioners Office (ICO). Data protection compliance within departments is delegated down to Access to Information Network (AIN) Representatives.
5. The objectives of this Internal Audit review are to verify that adequate arrangements are in place to help ensure that the CoL meets its GDPR obligations, as follows:
    - Staff have received training / guidance to help ensure that they are fully aware of their GDPR obligations.
    - Officers (AINs) have been appointed within departments to address and/or provide support on data protection issues.

- Self-Audit Monitor checklists are completed as required. Input/ evidence provided is subject to scrutiny and challenge. Action plans are developed to manage any control gaps.
- Personal data is only kept as required and for as long as necessary and in line with retention guidelines. Access to personal data is controlled and restricted to work needs. Data retention periods are applied automatically and routine checks undertaken within departments, to purge personal data no longer required.
- Record Retention Schedules are maintained and routine checks undertaken within departments, to purge personal records no longer required.
- Breaches are reported to the Central Compliance Team and onwards to the ICO if appropriate. Processes are put in place, if appropriate to help prevent a recurrence of the incident. The nature/number and type of incidents are reported to Committee.

6. Internal Audit sought to obtain assurance as to the adequacy of the internal control environment. The audit opinion is based upon discussions with key staff, examination of systems and the findings of sample testing, as such, our work does not provide an absolute assurance that material error, loss or fraud does not exist.

Assurance Statement

Assurance Level	Description
Moderate Assurance 'Amber'	An adequate control framework is in place but there are weaknesses and/or a lack of compliance which may put some system objectives at risk.

Recommendations	Red	Amber	Green	Total
Number Made:	0	4	0	4
Number Accepted:		4	0	4

Key Conclusions

Staff Training

7. **Completion of the online General Data Protection Regulation (GDPR) training module by staff is regularly monitored by the Compliance Team. As at 1 July 2019, 93.75% of staff had completed the GDPR training.**

8. **An issue was identified during testing within departments, that some members of staff had still not completed the GDPR training module after being issued with two reminders. An amber recommendation has been raised to address this issue (Recommendation 1).**

9. The CoL has a Data Protection Policy was last reviewed in April 2018. GDPR policies and guidance documents are available to staff on the intranet.

Access to Information Network (AIN) Representatives

10. Each City of London (CoL) department has one or more GDPR co-ordinators, who are also AIN Representatives. No issues were identified from testing within this area.

Self-Audit Monitor Checklists

11. Departments have completed quarterly Self-Audit Monitor checklists, which are collated by the Compliance Team in 'heat maps' which identify areas for future improvement. No issues were identified from testing within this area.

Access to Personal Data

12. An issue was identified from testing that the corporate 'W' drive (which can be accessed by all staff) contains a significant amount of obsolete data and personal data. An amber recommendation has been raised to address this issue (Recommendation 2).

13. A comprehensive information management review was carried out across the whole Corporation in 2018. Following the review, an Information Management Strategy was produced, containing a High Level Activities Plan.

Record Retention Schedules

14. It is not possible to provide assurance that record retention schedules are in place for all service areas; sample testing identified that record retention schedules for the Department of Markets and Consumer Protection and Department of Community and Children's Services were not yet finalised, although they were substantially complete. An amber recommendation has been raised to address this issue (Recommendation 3).

15. In addition, an issue has been identified that Departments have not been required to carry out regular checks on whether obsolete data is being deleted in accordance with record retention schedules. An amber recommendation has been raised to address this issue (Recommendation 4).

Data Security Breaches

16. The Compliance Team maintains a log of data security breaches notified by departmental staff. The log includes details of actions taken to prevent future similar breaches. Data breaches have been reported to the Information Commissioners Office as required. No issues were identified from our testing of this area.

SECTION B: AUDIT FINDINGS AND RECOMMENDATIONS

Staff Training

17. All CoL staff are required to complete a GDPR e-learning module to help ensure that they are aware of their responsibilities. The e-learning training module was launched on 23 April 2018. Some departments have staff who do not have access to the e-learning facility and receive alternative GDPR training (e.g. face-to-face training in workshops).

18. The Compliance Team produces a quarterly summary report which shows the number and percentage of staff in each department who have:
    - completed GDPR training;
    - have GDPR training in progress;
    - who have not yet started GDPR training; and
    - are exempted from GDPR training (e.g. due to maternity leave).

19. The quarterly summary report is emailed to all Chief Officers. The most recent report (dated 1 July 2019) showed that the overall completion level for GDPR training was 93.75%.

20. GDPR training statistics were submitted to the Audit and Risk Management Committee on 6 November 2018 and 12 March 2019.

21. Testing in the Department of Communities and Children's Services identified that 19 members of staff had not completed the GDPR training module despite having been issued with two reminders (Recommendation 1).

Priority	Issue	Risk
Amber	Audit testing identified members of staff who had still not completed the GDPR training module after being issued with two reminder emails.	Where staff do not complete GDPR training in a timely manner, there is a risk that they may not comply with the Data Protection Act 2018.
Recommendation 1: Where members of staff have not completed the GDPR training module after receiving two reminders, consideration should be given to introduction of a sanction e.g. temporary revocation of network access.		
Management Response and Action Plan Departments are chased on a quarterly basis with regards to chasing any members of staff who have not completed the training, and also when required. However, I note that we have maintained a high level of compliance, 93-94% (Completed, Exempt and Temporary Exempt), for the period April 2018 to date.		

Regarding, the recommendation of revoking access to those who have not completed the training, while this is good in practise, we consider that there could be difficulty in implementing this recommendation. As the reports received from learning pool, which form the basis of the outstanding chasers and statistics provided to chief officers and AIN reps, are often inaccurate and will not account for members of staff who have been made exempt for a variety of reasons. Additionally, these reports are also negatively impacted by staff turnover, with some members of staff being marked as exempt because they no longer work for the CoL and their city learning account has not been deleted, when the report is run.

Therefore, to revoke the access of staff members to the system as a result of non-completion would be a time-consuming exercise, requiring an additional review of the reporting mechanisms.

Responsibility: Departmental Managers supported by departmental AIN reps and the C&CS Information Compliance Team

Target Implementation Date: 31 March 2020 and ongoing thereafter

Further Comment from Internal Audit: noted that the action proposed by the Information Compliance Team will support improved completion of mandatory training for information management, there still exists a weakness around completion of mandatory training generally. This is out of scope for this review and so will be picked up within further audit work.

* Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided.

22. GDPR policies and guidance documents are available to staff on the intranet. The GDPR departmental co-ordinators advise staff when policies are updated.

Access to Information Network (AIN) Representatives

23. The Comptroller and City Solicitor was appointed as the CoL's Data Protection Officer (DPO) by the Policy and Resources Committee on 21 June 2017. The minimum duties of the DPO are defined in Article 39 of the GDPR.

24. Each CoL department has AIN Representatives whose responsibilities include compliance with the Data Protection Act 2018 and GDPR. One or more of the department's representatives is designated as the GDPR co-ordinator (for example, the Department of Markets and Consumer Protection has a single GDPR co-ordinator, whereas the Department of Community and Children's Services has separate co-ordinators for housing services and other services).

25. The AIN Representatives have received specialist GDPR training and receive updates on data protection issues via a newsgroup set up by the Compliance Team. An AIN Forum has been set up and has quarterly meetings.

Self-Audit Monitor Checklists

26. A Self-Audit Monitor checklist was introduced in October 2018 and is completed by each department on a quarterly basis. The checklist is based on the self-assessment checklist produced by the Information Commissioner's Office (ICO), and has a column for each service area within the department. Each compliance action on the checklist is Red, Amber, Green (RAG) rated for each service area.

27. Quarterly Self-Audit Monitor checklists completed by departments are collated on a 'heat map' by a Business Analyst in the central Compliance Team. There are separate 'heat maps' for phase one returns (higher risk departments) and phase two returns (lower risk departments).

28. The phase one 'heat map' submitted to the Audit and Risk Management Committee in March 2019 showed red ratings for four areas (updating Record of Processing Activities, consent for processing of personal data, GDPR compliant contracts and requests to access personal data) for some departments, but all of the red ratings had improved to amber or green on the updated 'heat map' produced in July 2019. The total number of amber ratings for high risk departments fell by 31% between March 2019 and July 2019.

Access to Personal Data

29. The CoL has a Data Protection Policy which was last reviewed in April 2018. The Policy includes a definition of personal data, a list of six data protection principles and a statement of how the CoL will demonstrate compliance with the six data protection principles.

30. Personal data is held on the corporate 'W' drive, departmental 'H' drives, One Drive and SharePoint. Access to folders on the 'H' drives is restricted to members of the relevant teams. Team members can restrict access to individual files by password protection as required. Personal data is also held on databases which have restricted access.

31. The corporate 'W' drive was designed to facilitate file transfers between officers and was not intended to be a permanent repository for information, but it was established that the 'File Transfer' folder on the 'W' drive currently contains over 3,500 sub-folders, some of which relate to members of staff who have now left the CoL. Some of these sub-folders are likely to contain sensitive data, which could be accessed by any CoL staff.

32. Discussions with departmental GDPR co-ordinators established that efforts are made to identify and delete obsolete files on the 'W' drive where

possible, but this is difficult because files are not grouped by departments. It is noted that the Deputy IT and Head of Business Change and Engagement are due to submit a proposal for the management of the 'W' drive to the Summit Group (Recommendation 2).

Priority	Issue	Risk
Amber	The corporate 'W' drive (which can be accessed by all staff) contains obsolete data and personal data which has unrestricted access.	Where obsolete data is held, or where staff have unrestricted access to personal data (including sensitive data), there are risks of serious data security breaches and failure to comply with the Data Protection Act 2018.
Recommendation 2: All data permanently held on the 'W' drive should be reviewed as a matter of urgency and either deleted or transferred to a more secure location. Staff should be given clear instructions on future use of the 'W' drive.		
Management Response and Action Plan The 'W' drive was created as a cross-department information storage area to enable departments to share information before the Corporation adopted Sharepoint, which otherwise would have been stored and duplicated across individual department (H) drives. However, without the relevant guidance, policy and controls in place, and given that this storage area has no identified owner(s), this has become a significant risk to the Corporation. Due to the lack of clarity, volume, age, accuracy and relevance of the information within the W drive, combined with the lack of policy and security controls, the Corporation agrees that this should be addressed urgently. Analysis has taken place by IT to ascertain filetypes within that area, but this does not identify personal information or information which is incorrectly stored there. To this end, market discovery work was carried out in to ascertain if automated information discovery tools exist with the capability to identify personal data to enable improved identification, location, handling and retention. However, this was expensive (minimum £80k+ for the cheapest) and no funding was available in-year to fund this. The Information Management Board (IMB) agreed on 29th October to take accelerated steps to mitigate the risk the W drive poses to the Corporation.		

A joint Comptrollers and IT plan will be developed with the purpose of removing the W drive and moving the required content to alternative storage locations within a timeline of 5 months from approval from the relevant officer groups and member Committees.

This will include:

1. A documented plan to take to Boards and Committees to gain approval for this work.
2. An "information amnesty" where the W will be made read-only to ensure that no new information is stored there, for a period of 3 months.
3. A communication and guidance campaign explaining the reasons why the IMB have taken this decision and providing guidance on where the various information types should be stored within the Corporation's information storage areas (primarily OneDrive and Sharepoint.)
4. Deletion of the W drive and what information remains at the end of this amnesty period.

Responsibility: IT Director and Comptroller and City Solicitor

Target Implementation Date: March 2020, assuming approval.

* Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided.

33. The Summit Group approved a comprehensive information management review across the whole CoL in October 2017. The review identified that the CoL kept too much information, often in "obscure silos", and also highlighted that information was often unstructured, duplicated or out-of-date. The review also identified a risk of information breaches leading to regulatory sanctions and bad publicity.

34. A new Information Management Strategy was produced as a result of the review (containing a High-Level Activities Plan), supported by an Information Management Policy and refreshed Records Management Policy. Implementation of the Information Management Strategy is being overseen by the Digital Task and Finish Group and Information Governance Group.

Record Retention Schedules

35. Each departmental GDPR co-ordinator has developed a 'Record of Processing Activities' (RoPA) following an information audit. Each

department also has a departmental record retention schedule which is based on the corporate record retention schedule but is considerably more detailed.

36. Testing of record retention schedules in a sample of departments identified that schedules for the Department of Markets and Consumer Protection and Department of Community and Children's Services were not yet finalised, although they were substantially complete (Recommendation 3).

Priority	Issue	Risk
Amber	Sample testing identified that record retention schedules for the Department of Markets and Consumer Protection and Department of Community and Children's Services have not yet been finalised.	Record retention schedules may be similarly incomplete for other service areas. Where record retention schedules are not finalised, there is a risk that data may not be managed correctly or deleted when it reaches its expiry date.
Recommendation 3: The Compliance Team should ensure that, specifically, record retention schedules for the Department of Markets and Consumer Protection and Department of Community and Children's Services are finalised in a timely manner. More widely, that there is an appropriate mechanism to ensure that schedules are in place across the organisation, including an escalation process to deal with exceptions.		
Management Response and Action Plan Good progress continues to be made regarding the implementation of record retention schedules. With most departments having implemented their own schedules or are implementing the overarching CoL Records Management Schedule. Further we note that the retention schedules are monitored as part of the self-audit monitors, undertaken by departments on a quarterly basis. However, we plan to monitor this further as part of our internal compliance checks. Responsibility: Departmental Managers, supported by departmental AIN reps and the C&CS – Information Compliance team Target Implementation Date: 31.12.2020 * Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided.		

37. The CoL's Data Protection Policy states that the CoL will ensure that data is only kept for as long as necessary in accordance with the retention schedules. Discussions with departmental GDPR co-ordinators identified

that service managers are responsible for ensuring that obsolete personal data is deleted when it reaches its expiry date.

38. Implementation of disposal dates in record retention schedules is at various stages. For example, it was established that obsolete data cannot be deleted from the corporate finance system (CBIS), and no data has yet been deleted from the integrated payroll and human resources system (City People).

39. Departments have not been required to carry out regular checks on whether obsolete data is being deleted in accordance with record retention schedules. The Department of Community and Children's Services has carried out local operational compliance checks, which included checks on physical locking of laptops, laptops logged on whilst unattended, compliance with the department's clear desk policy and physical security over confidential paper files. However, these checks did not include compliance with record retention schedules (Recommendation 4).

Priority	Issue	Risk
Amber	Local operational compliance checks in departments have not been carried out in all departments on a regular basis. The checks carried out did not cover compliance with record retention schedules.	Where compliance with disposal dates specified in record retention schedules is not regularly monitored, there is an increased risk that obsolete data will continue to be retained, resulting in failure to comply with the Data Protection Act 2018.
Recommendation 4: The Compliance Team should introduce new arrangements for local operational compliance checks. Each department should be required to carry out regular checks, which should include compliance with disposal dates for categories of data specified in record retention schedules. Results of the checks should be notified to the Compliance Team. The Compliance Team should follow up instances where required checks have not been carried out by the due date.		
Management Response and Action Plan Compliance Checks were put on hold since 2017, due to the implementation of GDPR/DPA 2018 and while the Information Compliance Team were under resourced, due to staff leaving and then recruiting and training new team members. Now we are fully resourced again, we will be looking to implement new compliance checks, which incorporate all aspects of the DPA 2018 and more specifically the implementation of record retention schedules.		

Responsibility: Departmental AIN Reps and the C&CS Information Compliance Team

Target Implementation Date: 31.12.2020

* Where recommendation not accepted indicate alternative action that will be taken to mitigate risk or reasoning for accepting risk exposure to be provided.

Data Security Breaches

40. The CoL's People Security Policy states that any information security incident must be reported using the Security Incident Tracker available on the intranet. A standard 'Internal Notification of a Data Security Breach' form is completed for each suspected breach.

41. The Compliance Team maintains a log of data security breaches notified by staff; there is a separate log for each calendar year. The 2019 log shows that 44 data security breaches were reported to the Compliance Team between 1 April and 30 July 2019. Two of these breaches were reported to the ICO.

42. Discussions with departmental GDPR co-ordinators identified that staff had a good understanding of the need to notify suspected data security breaches.

43. In April 2019, the Compliance Team carried out a detailed review of the seven most significant recent data security breaches, and confirmed that appropriate action was taken in respect of each breach (e.g. notification to the ICO where applicable, provision of training to staff and amendments to procedures).

44. The Compliance Team analyses notified data security breaches by department and root cause. Quarterly statistics on data security breaches are submitted to the Corporate Strategy and Performance Department.

45. Recent data security breaches are discussed at each quarterly AIN Forum meeting.

46. The Audit and Risk Management Committee agreed on 12 March that it would receive GDPR monitoring reports including information on data security breaches three times a year. The reports are also received by the Digital Services Sub (Finance) Committee.

APPENDIX 1: AUDIT DEFINITIONS AND RESPONSIBILITIES

Assurance levels

Category	Definition
Nil Assurance 'Dark Red'	There are fundamental weaknesses in the control environment which jeopardise the achievement of system objectives and could lead to significant risk of error, fraud, loss or reputational damage being suffered.
Limited Assurance 'Red'	There are a number of significant control weaknesses and/or a lack of compliance which could put the achievement of system objectives at risk and result in error, fraud, loss or reputational damage.
Moderate Assurance 'Amber'	An adequate control framework is in place but there are weaknesses and/or a lack of compliance which may put some system objectives at risk.
Substantial Assurance 'Green'	There is a sound control environment with risks to system objectives being reasonably managed. Any deficiencies identified are not cause for major concern.

Recommendation Categorisations

Priority	Definition	Timescale for taking action
Red - 1	A serious issue for the attention of senior management and reporting to the appropriate Committee Chairman. Action should be initiated immediately to manage risk to an acceptable level.	Less than 1 month or more urgently as appropriate
Amber - 2	A key issue where management action is required to manage exposure to significant risks, action should be initiated quickly to mitigate the risk.	Less than 3 months
Green - 3	An issue where action is desirable and should help to strengthen the overall control environment and mitigate risk.	Less than 6 months

Note:- These 'overall assurance level' and 'recommendation risk ratings' will be based upon auditor judgement at the conclusion of auditor fieldwork. They can be adjusted downwards where clear additional audit evidence is provided by management of controls operating up until the point of issuing the draft report.

What Happens Now?

The final report is distributed to the relevant Head of Department and the relevant Heads of Service.

A synopsis of the audit report is provided to the Chamberlain, relevant Members, and the Audit & Risk Management Committee. Internal audit will carry out a follow-up exercise of the high priority (red and amber) recommendations quarterly, timed to provide an update to Committee, after the issue of the final audit report. The ongoing progress in implementing each recommendation is reported by Internal Audit to each meeting of the Audit & Risk Management Committee.

Any Questions?

If you have any questions about the audit report or any aspect of the audit process please contact Miyako Graham, Audit Manager – Mazars on 07825 450782, or via email to miyako.graham@mazars.co.uk. Alternatively, please contact Matt Lock, Head of Audit & Risk Management via email to matt.lock@cityoflondon.gov.uk.