

Final Internal Audit Report

GDPR

May 2019

Distribution: Interim Executive Director Resources (Final only)
Interim Director Law & Governance
Head of Litigation and Corporate Law (Data Protection Officer)
Data Protection (GDPR) Project Manager

Assurance Level	Recommendations Made	
Substantial Assurance	Priority 1	0
	Priority 2	2
	Priority 3	0

Confidentiality and Disclosure Clause

This report ("Report") was prepared by Mazars LLP at the request of London Borough of Croydon and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit of London Borough of Croydon and to the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, re-interpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, re-interpretation, amendment and/or modification by any third party is entirely at their own risk.

Please refer to the Statement of Responsibility in Appendix 3 of this report for further information about responsibilities, limitations and confidentiality.

Contents

Page

Executive Summary

1. Introduction.....	2
2. Key Issues.....	2

Detailed Report

3. Actions And Key Findings/Rationale	3
---	---

Appendices

1. Terms Of Reference
2. Definitions For Audit Opinions And Recommendations
3. Statement Of Responsibility

1. Introduction

- 1.1 The law relating to data protection changed on 25 May 2018, with the Data Protection Act 2018 coming into force. This incorporates the General Data Protection Regulation (GDPR) and replaced the Data Protection Act 1998. Although many of the principles will remain the same as the DPA 1998, there are some important changes which affect the London Borough of Croydon.
- 1.2 In general terms, GDPR places more emphasis on transparency, accountability and record keeping, and it is important that personal data is handled correctly as the Information Commissioner's Office (ICO), can issue fines to organisations that breach GDPR (up to €20 million or 4% of annual turnover, whichever is higher).
- 1.3 The final GDPR Implementation Plan from December 2018 still includes some areas with an Amber status, but in each of these cases, a plan had been set out to complete the work as part of the post project work. In addition, the Project Board Closure Report stated that the progress on outstanding issues will be reported to the Governance Board or Information Management Steering Group (IMSG) at regular intervals.
- 1.4 The updated staff Code of Conduct was published by individual email to all staff with supported e-learning on 1st March 2019. It was noted that this new version includes amendments in relation to both GDPR and social media usage.
- 1.5 This audit was undertaken as part of the agreed Internal Audit Plan for 2018/19.

2. Key Issues

Priority 2 Issues

The Information Management section of the Council's intranet includes a guidance and policy section, within which all policies are out of date. It also includes the link to the GDPR section, which contains the up-to-date GDPR policies, training webinars and podcasts, IAR requirements etc. Therefore staff members could logically assume that the old policies are still relevant. Furthermore, the Council's Data Breach Procedures were not dated. **(issue 1)**

At the time of audit there were no plans in place to check staff knowledge and remind them about the requirements of GDPR. In addition, ongoing compliance checks had not yet commenced and we were unable to obtain information on how these would be carried out. **(Issue 2).**

There were no Priority 3 issues.

3. Actions and Key Findings/Rationale

Control Area 2: Information Management Policies and Procedures		Detailed Finding/Rationale – Issue 1
Priority	Action Proposed by Management	Expected Control
2	<p>The Information Management Team is currently reviewing in conjunction with the Communications Team and Web team the Information Management Page with a view to rationalizing the content of both the intranet and internet pages, to update and/or remove broken and outdated links, to remove out of date policies and to make the content more accessible. This work is ongoing, and has several dependencies with the work underway in Digital Services involving refreshing the digital offering to our residents.</p> <p>The links in relation to the Internet are now updated.</p> <p>In terms of the Intranet some work is commenced with the Comms team to identify old links and these will be removed by the end of May 2019 in terms of the GDPR pages.</p> <p>The proposal in terms of the IT policies, responsibility for these is split with the Croydon digital Team as this incorporates policies owned by CDS. The information team will be writing new policies for the area's that will fall into the remit of the team by the end of July.</p>	<p>Expected Control</p> <p>All Information Security Policies and Procedures should have been updated to comply with GDPR.</p> <p>Issue/Finding</p> <p>A link to the up to date security policies on the intranet was provided, but the page that it links to was very difficult to read and navigate.</p> <p>A search for "IT Policy" on the Intranet directs users to the Information Management - Guidance and Policy Documents page. All policies on this page were out of date and most had last been reviewed in 2012. Examination of a sample of policies for this page found that the Records Retention Policy, IT Access Policy, Data Destruction Policy and Remote Working Policy were all last reviewed in 2012 and the Information Security Policy was undated (but referred to DPA 1998).</p> <p>It was also noted that the Council's Data Breach Procedures were undated.</p> <p>It was further noted that the Information Management section also included the link to the GDPR section, which includes the up-to-date GDPR policies, training webinars and podcasts, IAR requirements etc. Therefore staff members could logically assume that the old policies are still relevant.</p> <p>Risk</p> <p>Where out of date policies are published alongside current guidance and where policies are undated, employees may not follow appropriate processes that support GDPR compliance or may be unclear about what to do or who to contact causing delay in the response to any incidents.</p>

	Council's data breach procedure will be replaced with the current version (which is review dated) by the end of April.		
Responsible officer	Deadline		
Legal Service Business Manager / Business Manager Croydon Digital Service	October 2019		

Control Area 4: Monitoring GDPR Compliance	
Priority	Action Proposed by Management
2	<p>The Information Management Team are liaising with L&D with a view to designing an appropriate method to check/refresh staff knowledge of GDPR. Consideration will be given as to whether refresher training or an annual knowledge check could be created, similar to the Equality & Diversity training.</p> <p>The appropriate method for the refresher training will be identified by the end of April. Implementation is dependent upon cross dependencies with CDS but is scheduled for the end of July.</p>
Detailed Finding/Rationale – Issue 2	
<p>Expected Control</p> <p>Article 39(1)(b) of the General Data Protection Regulation (GDPR) states that it is the responsibility of the Data Protection Officer to “(b) monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits”.</p> <p>The Data Protection Act 2018 has two categories for breaches of GDPR, acts deemed to be a lesser breach hold a maximum fine of €10 million or two per cent of a company’s annual revenue, whichever is greater, and for more severe breaches, the maximum fine is €20 million or four per cent of a company’s annual revenue, whichever is greater.</p> <p>Issue/Finding</p> <p>96% of Council staff have recently completed e-learning training for GDPR, which is also now mandatory for new staff. Going forward, the DPO is considering devising a scheme where staff must answer GDPR related questions before logging into their computer in order to check staff knowledge and remind them about the requirements of GDPR. However, there were no formal plans for this that could be evidenced at the time of the audit.</p> <p>It was noted that Information Champions were in place across the Council and were intended to be a first point of contact for their relevant service/department area for information management concerns, queries or suggestions, including GDPR queries. They are also intended to be responsible for ensuring and monitoring staff GDPR compliance.</p> <p>However, ongoing compliance checks have not yet commenced and we were unable to obtain information on what form this would take.</p> <p>Risk</p> <p>Where the Council does not implement methods of reinforcing staff knowledge and checking compliance levels with regards to GDPR, there is a risk that non-compliance may go undetected, making the Council liable to fines and/or reputational damage.</p>	
Responsible officer	Deadline
Legal Service Business Manager	End of July 2019

TERMS OF REFERENCE

GDPR

1. INTRODUCTION

- 1.1 The law relating to data protection changed on 25 May 2018, with the Data Protection Act 2018 coming into force. This incorporates the General Data Protection Regulation (GDPR) and replaced the Data Protection Act 1998. Although many of the principles will remain the same as the DPA 1998, there are some important changes which affect the London Borough of Croydon.
- 1.2 In general terms, GDPR places more emphasis on transparency, accountability and record keeping, and it is important that personal data is handled correctly as the Information Commissioner's Office (ICO), can issue fines to organisations who breach GDPR (up to €20 million or 4% of annual turnover, whichever is higher).
- 1.3 The purpose of this audit is to assess how the compliance of the London Borough of Croydon with these changes.
- 1.4 This audit is part of the agreed Internal Audit Plan for 2018/19.

2. OBJECTIVES AND METHODOLOGY

- 2.1 The overall audit objective is to provide an objective independent opinion on the adequacy and effectiveness of controls/processes relating to the Coroner's Service.
- 2.2 The overall audit objective is to provide an objective independent opinion on the adequacy and effectiveness of controls / processes.
- 2.3 The audit will for each controls / process being considered:
- Walkthrough the processes to consider the key controls;
 - Conduct sample testing of the identified key controls, and
 - Report on these accordingly.

3. SCOPE

- 3.1 This audit examined the Council's arrangements for the following areas relating to GDPR (and number of recommendations made):





Control Areas/Risks	Recommendations Made		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Organisational, Management and Legislative Requirements	0	0	0
Policies and Procedures	0	1	0
Roles and Responsibilities	0	0	0
Organisational Awareness and Training	0	1	0

Data Documentation, Classification and Management	0	0	0
Confidentiality, Integrity and Availability of Data	0	0	0
Third Parties	0	0	0
Legal Basis/ Consents	0	0	0
Monitoring and Reporting	0	0	0

DEFINITIONS FOR AUDIT OPINIONS AND RECOMMENDATIONS

In order to assist management in using our reports:

We categorise our **audit assurance opinion** according to our overall assessment of the risk management system, effectiveness of the controls in place and the level of compliance with these controls and the action being taken to remedy significant findings or weaknesses.

	Full Assurance	There is a sound system of control designed to achieve the system objectives and the controls are consistently applied.
	Substantial Assurance	While there is basically a sound system of control to achieve the system objectives, there are weaknesses in the design or level of non-compliance which may put this achievement at risk.
	Limited Assurance	There are significant weaknesses in key areas of system controls and/or non-compliance that puts achieving the system objectives at risk.
	No Assurance	Controls are non-existent or weak and/or there are high levels of non-compliance, leaving the system open to the high risk of error or abuse which could result in financial loss and/or reputational damage.

Priorities assigned to recommendations are based on the following criteria:

Priority 1 (High)	Fundamental control weaknesses that require the immediate attention of management to mitigate significant exposure to risk.
Priority 2 (Medium)	Control weakness that represent an exposure to risk and require timely action.
Priority 3 (Low)	Although control weaknesses are considered to be relatively minor and low risk, action to address still provides an opportunity for improvement. May also apply to areas considered to be of best practice.

STATEMENT OF RESPONSIBILITY

We take responsibility to the London Borough of Croydon for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

Registered office: Tower Bridge House, St Katharine's Way, London E1W 1DD, United Kingdom.
Registered in England and Wales No 0C308299.