

Dacorum Borough Council

Final Internal Audit Report

GDPR

August 2018

This report has been prepared on the basis of the limitations set out on page 10.

CONFIDENTIAL

Distribution List:

John Worts – Information Security Manager
Mark Brookes – Solicitor to the Council
Matt Rawdon – Group Manager, People and Performance
Linda Roberts – Assistant Director, Performance, People and Innovation
Nigel Howcutt – Assistant Director, Finance & Resources
James Deane – Corporate Director (Finance and Operations) (Final Report Only)
Sally Marshall – Chief Executive (Final Report only)

Key Dates:

Date of fieldwork: July/August 2018
Date of draft report: August 2018
Receipt of responses: August 2018
Date of final report: August 2018

Status of our reports

This report ("Report") was prepared by Mazars LLP at the request of Dacorum Borough Council 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 Dacorum Borough Council 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, reinterpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk. Please refer to the Statement of Responsibility in Appendix C of this report for further information about responsibilities, limitations and confidentiality.

Contents

| | |
|---|----------|
| 1. Executive Summary | 1 |
| 2. Scope of Assignment | 3 |
| 3. Assessment of Control Environment..... | 4 |
| 4. Observations and Recommendations | 5 |
| Recommendation 1: Framework to be implemented for conducting Privacy Impact Assessments in line with the guidance on such processes contained in GDPR (Priority 2). | 5 |
| Recommendation 2: All staff to complete mandatory training (Priority 2). | 6 |
| Recommendation 3: Scope for the Incident Management Policy to be updated with a flowchart to help staff to understand processes to follow in the event of an incident (Priority 3). | 7 |
| Appendix A - Reporting Definitions | 8 |
| Appendix B - Staff Interviewed..... | 9 |
| Appendix C Statement of Responsibility | 10 |

1. Executive Summary

1.1. Background

As part of the Internal Audit Plan for 2018/2019 we have been requested to undertake a review of Dacorum Borough Council's key control and processes for the General Data Protection Regulation (GDPR).

This area was included in the plan at request of the Audit Committee and also due to significance of risks related to the area in Dacorum Borough Council's Risk Register.

In April 2016, the European Union introduced GDPR. This legislation is intended to strengthen data protection rights for individuals within the EU and came into effect on 25th May 2018.

This legislation also applies to organisations outside the EU that offer goods or services to individuals within the EU. The UK government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

We are grateful to the Corporate Director (Finance and Operations), Assistant Director (Performance, People and Innovation), the Information Security Manager and other council staff for their assistance provided to us during the course of the audit.

This report summarises the results of the internal audit work and, therefore does not include all matters that came to our attention during the audit. Such matters have been discussed with relevant staff.

1.2. Audit Objective and Scope

The overall objective of the audit was to evaluate and test controls over the following areas:

- An assessment of plans in place to address GDPR that came into force in May 2018;
- Assessment of action plan(s) in place to comply with the new regulation to ensure that any gaps are covered to new rules; and
- Responsibility for delivery and governance of the GDPR project.

The audit also included a review of key areas stipulated within Article 5 of GDPR, which requires 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 personal data.

Although the UK has had data protection legislation since the Data Protection Act 1984 came into force, the demands on the Council have increased since 25 May 2018 when new GDPR legislation came into force. In order to ensure ongoing compliance with data protection legislation there is an Information Security manager (Data Protection Officer) who oversees management and control of data.

Further detail on scope of the audit is provided in Section 2 of the report.

1.3. Summary Assessment

Our audit of DBC's internal controls in operation found that, whilst there is a basically sound system of internal control design, there are weaknesses in design which may place some of the system objectives at risk. There is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

Our assessment in terms of the design of, and compliance with, the system of internal control covered is set out below:

| Evaluation Assessment | Testing Assessment |
|-----------------------|--------------------|
| Substantial | Substantial |

Management should be aware that our internal audit work was performed according to UK Public Sector Internal Audit Standards (PSIAS) which are different from audits performed in accordance with International Standards on Auditing (UK and Ireland) issued by the Auditing Practices Board. Similarly, the assurance gradings provided in our internal audit report are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board.

The classifications of our audit assessments and priority ratings definitions for our recommendations are set out in more detail in Appendix A, whilst further analysis of the control environment is shown in Section 3.

1.4. Key Findings

Two priority 2 recommendations and one priority 3 recommendation were raised where we believe there is scope for improvement within the control environment. These are set out below:

- Framework to be implemented for conducting Privacy Impact Assessments in line with the guidance on such processes contained in GDPR (Priority 2).
- All staff to complete GDPR mandatory training (Priority 2).
- Incident Management Policy to be updated with a workflow document (Priority 3).

Full details of the audit findings and recommendations are shown in Section 4 of the report.

1.5. Management Response

The management response was received in a timely manner and has been included in the main body of the report.

1.6. Acknowledgement

We would like to take this opportunity to thank all staff involved for their time and co-operation during the course of this visit.

2. Scope of Assignment

2.1. Background

As part of the agreed 2018/2019 Audit Plan, Mazars have undertaken a review of the controls in place at Dacorum Borough Council in relation to GDPR.

2.2. Scope of the Audit

The audit was carried out to evaluate and test controls over the following areas:

- An assessment of plans in place to address GDPR that came into force in May 2018:

The Council has an established data protection policy and a project plan in place, which has been used to identify requirements for the Information Security Manager to manage the GDPR project.

There is a document centre accessible by all staff on the council intranet, which includes all GDPR, Information and Security policies.

- Assessment of action plan(s) in place to comply with the new regulations to ensure that any gaps are covered to the new set of rules:

Information asset registers are currently being updated and all required documentation under GDPR which was already in place, is being updated or will be drafted as per the GDPR project plan.

The Housing department has adopted an enhanced GDPR regime within their department and have unofficial GDPR champions to help staff to maintain compliance. The team also updated their personal development plans to incorporate GDPR. The DPO is using the service as a model for all services to follow.

- Responsibility for delivery and governance of the GDPR project:

There has been an established GDPR awareness campaign across the organisation. This has also included the council's Corporate Management Team, Senior Leadership Team, Elected Representatives including Audit Committee, Parish Councils and Community Associations.

The council has updated the Strategic Risk Register to highlight the implications of breaching GDPR and penalties the council face in light of that. An amber risk score has been assigned.









The audit approach was developed by an assessment of risks and management controls operating within each area of the scope. The following procedures will be adopted:

- Identification of the role and objective of each area;
- Identification of risks relating to the auditable area and the controls in place that enable the control objectives to be achieved; and
- Evaluation and testing of controls within the system.

3. Assessment of Control Environment

The following table sets out in summary the control objectives we have covered as part of this audit, our assessment of risk based on the adequacy of controls in place, the effectiveness of the controls tested and any resultant recommendations.

The classifications of our assessment of risk for the design and operation of controls are set out in more detail in Appendix A.

| Control Objectives Assessed | Design of Controls | Operation of Controls | Recommendations Raised |
|--|---|--|------------------------------|
| An assessment of plans in place to address GDPR that came into force in May 2018 |  |  | |
| Assessment of action plan(s) in place to comply with the new regulations to ensure that any gaps are covered to the new set of rules |  |  | Recommendation 1 (P2) |
| Responsibility for delivery and governance of the GDPR project |  |  | Recommendation 2 (P2) |
| Assessment of delivery of the GDPR awareness campaign across the organisation |  |  | Recommendation 3 (P3) |

The classifications of our assessment of risk for the design and operation of controls are set out in more detail in Appendix A.

4. Observations and Recommendations

Recommendation 1: Framework to be implemented for conducting Privacy Impact Assessments in line with the guidance on such processes contained in GDPR (Priority 2).

| |
|---|
| <p>Recommendation</p> <p>The Council should develop a privacy by design approach to working and embedding the appropriate technical, administrative and physical safeguards required to comply with GDPR.</p> <p>The Privacy Impact Assessment (PIA) should be embedded within Project management framework and risk management process.</p> <p>For any new projects, a PIA should be undertaken to establish the potential impact on data protection/GDPR compliance.</p> |
| <p>Observation</p> <p>The Council has not implemented a framework to allow them to identify instances where a privacy impact assessment would be required and how this would be performed in the event that an assessment should be undertaken.</p> <p>Without implementing a framework for conducting privacy impact assessments, there is an increased risk that the Council will fail to comply with GDPR requirements regarding Data Protection by Design and Data Protection Impact Assessments. This in turn could result in breaches of the new Act and ensuing litigation and reputational damage.</p> <p>The Council has carried out one off PIA's, but there is not a specific process in place for officers to carry out.</p> |
| <p>Responsibility: Information Security Manager / Innovation & Improvement Team Leader</p> |
| <p>Management response / deadline: Agreed. DPIA will be part DBC's Project Management framework by 30/9/18.</p> |

Recommendation 2: All staff to complete mandatory training (Priority 2).

| |
|--|
| <p>Recommendation</p> <p>An appropriate process should be introduced to capture all staff that have undertaken GDPR Training.</p> <p>It should be ensured that all staff have completed Mandatory GDPR training as soon as practicably possible.</p> |
| <p>Observation</p> <p>Staff GDPR training figures were provided at the time of the audit from the HR system, the DPO. This showed that although over 700 staff work at the council, but only just over 400 were shown on table sent.</p> <p>As a result:</p> <ul style="list-style-type: none"> • A significant number of staff have not completed the mandatory training and/or • The training statistics on the HR system are inaccurate. |
| <p>Responsibility: HR and Information Security Manager</p> |
| <p>Management response / deadline: Note the figures (for 1 August 2017 to 30 July 2018) for Forum staff attending were 483. The discrepancy lies only with mainly manual working / outdoor working staff from Cupid Green attending. We will try to obtain the figures for Cupid Green Staff, Deadline by 31/10/18.</p> |





Recommendation 3: Scope for the Incident Management Policy to be updated with a flowchart to help staff to understand processes to follow in the event of an incident (Priority 3).

| |
|---|
| <p>Recommendation</p> <p>The incident management policy should be updated and a flowchart attached as per the data breach policy, helping and enabling staff to effectively detect, report and investigate a personal data breach.</p> |
| <p>Observation</p> <p>There is a Data Breach policy in place and accessible via the intranet. There is also a workflow document to help staff understand what to do in the event of a breach.</p> <p>There is also an IT incident management policy for staff to follow in the event of an IT/virus failure.</p> <p>Both policies have similar messages for staff, and the data breach policy has an easy to read workflow document which (in the event of an incident) staff could easily apply.</p> <p>It was felt that it would also be useful for the incident management policy to be updated with a workflow diagram to enable staff to follow the process more clearly.</p> |
| <p>Responsibility: ICT in conjunction with Information Security Manager</p> |
| <p>Management response / deadline: Agreed – by 30/9/18</p> |

Appendix A - Reporting Definitions

Audit assessment

In order to provide management with an assessment of the adequacy and effectiveness of their systems of internal control, the following definitions are used:

| Level | Symbol | Evaluation Assessment | Testing Assessment |
|--------------------|---|--|---|
| Full |  | There is a sound system of internal control designed to achieve the system objectives. | The controls are being consistently applied. |
| Substantial |  | Whilst there is a basically sound system of internal control design, there are weaknesses in design which may place some of the system objectives at risk. | There is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk. |
| Limited |  | Weaknesses in the system of internal control design are such as to put the system objectives at risk. | The level of non-compliance puts the system objectives at risk. |
| Nil |  | Control is generally weak leaving the system open to significant error or abuse. | Significant non-compliance with basic controls leaves the system open to error or abuse. |

The assessment gradings provided here are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board and as such the grading of 'Full' does not imply that there are no risks to the stated control objectives.

Grading of recommendations

In order to assist management in using our reports, we categorise our recommendations according to their level of priority as follows:

| Level | Definition |
|---------------------------------------|--|
| Priority 1 | Recommendations which are fundamental to the system and upon which the organisation should take immediate action. |
| Priority 2 | Recommendations which, although not fundamental to the system, provide scope for improvements to be made. |
| Priority 3 | Recommendations concerning issues which are considered to be of a minor nature, but which nevertheless need to be addressed. |
| System Improvement Opportunity | Issues concerning potential opportunities for management to improve the operational efficiency and/or effectiveness of the system. |

Appendix B - Staff Interviewed

The following personnel were consulted:

Audit sponsor: Nigel Howcutt – Assistant Director, Finance & Resources

Audit Contacts: Matt Rawdon – Group Manager, People and Performance

- Assistant Director - Performance, People and Innovation
- Information Security Manager
- ICT Operations Team Leader
- Housing Team (Property & Place)

We would like to thank the staff involved for their co-operation during the audit.

Appendix C Statement of Responsibility

We take responsibility to Dacorum Borough Council 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.