GDPR Compliance

City of York Council

Internal Audit Report 2018/19

Business Unit: Corporate and Cross-Cutting
Responsible Officer: Interim Assistant Director – Legal and Governance
Service Manager: Information Governance & Feedback Team Leader
Date Issued: 8 July 2019
Status: Final
Reference: 10380/001

	P1	P2	P3
Actions	**0**	**9**	**1**
Overall Audit Opinion	Reasonable Assurance		

Summary and Overall Conclusions

Introduction

On 23 May 2018, the Data Protection Act 2018 (DPA) became UK law, repealing and replacing the 1998 Act. The DPA implements the EU's General Data Protection Regulation (GDPR), which came into force on 25 May, and provides for certain permitted derogations, additions and UK-specific provisions.

The main changes brought about with the introduction of the GDPR include the strengthening of the conditions for consent, enhanced rights for data subjects, the express requirement for privacy by design, greater enforcement powers and an increase in the maximum fine to the greater of €20 million or 4% of global turnover.

The council continually processes personal data in order to plan, run and improve its services, to perform its statutory duties, to carry out its regulatory, licensing and enforcement roles, to make payments, administer benefits and identify fraud and to improve the health of the population it serves. Where the council does not directly provide a service it also passes personal data on to the organisations that do if it is necessary for the performance of that service. With the council being such a large and complex organisation, it is crucial that it has sufficient measures in place to ensure its ongoing compliance with the GDPR and DPA both as a data controller and a data processor.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that procedures and controls within the system will ensure that:

- Appropriate policies and procedures are in place and these are sufficient to fulfil the requirements of the GDPR
- Staff have been made adequately aware of their responsibilities under the GDPR and trained where appropriate
- Effective oversight and governance arrangements are in place to monitor ongoing compliance and direct compliance efforts

The audit has not included a review of records management processes. This will instead be reviewed as a separate audit, to be carried out in 2019-20.

Key Findings

The council does not currently have a published policy statement which sets out how it achieves compliance with data protection legislation as a data controller. Some internal guidance is available to staff but a full suite of procedures, covering the activities required under the GDPR, has not yet been produced.

An application has been developed on which the council's Information Asset Register (IAR) is held. This is accessible to staff via the intranet and was found to be compliant with the requirements of Article 30 of the GDPR (records of processing activities). Given the extent of data processing undertaken by the council, it is not possible to provide assurance as to the completeness of the IAR in respect of the information assets actually in existence but some issues were observed with the completeness of individual records.

The council has a privacy notice covering its general data processing activities on its website. It has also made a number privacy notices available for service areas and specific information assets. However, the majority of service areas represented in the IAR do not have a privacy notice. It is likely that privacy information will be provided to service users in other formats but there has been no specific exercise undertaken by the council to match service area data processing to available privacy information and so assurances cannot be given that data subjects have been suitably informed about how their data is processed.

The Aptean Respond system, maintained by the Information Governance and Feedback team, allows for the logging and tracking of individual requests made under the rights of individuals. These requests are subject to the same one calendar month timescale (unless extended in cases of exceptional complexity or where multiple requests have been received from the same individual) and appropriate reminders have been scheduled in the system to monitor progress. The Aptean Respond system also serves as the council's log of data security incidents and was found to provide all necessary information to understand the source and nature of the incident, the timeliness with which it was responded to and the results of any investigation undertaken internally or by the ICO (including the subsequent tracking of any recommendations agreed). The data security incident reporting process, if followed, should allow for timely and appropriate notification to the ICO.

The council is signed up to the North Yorkshire Multi-Agency Information Sharing Protocol (MAISP) which enforces standards for the drawing up of information sharing agreements between signatories. The council has access to the Information Sharing Gateway (an application to manage information sharing agreements) which should further standardise the process of completing and reviewing information sharing agreements. However, the implementation of this process has been delayed and arrangements for completion of agreements with other third parties (i.e. those not in the MAISP) are not currently formalised.

A standard GDPR clause and schedule has been developed for inclusion in all contracts where personal data is being processed by a third party. Legal Services worked in conjunction with contract managers to identify existing contracts to be varied. These were then compiled into priority lists for completion but the Legal Services GDPR compliance document shows only very few of the priority contracts have been varied to include the new clause and schedule.

Briefing sessions were held with the council's Corporate Leadership Group[1] and other groups (on request) prior to the implementation of the GDPR. However, owing to the retirement of the previous training platform (iComply) and the time taken to make the GDPR module on the current training platform (MyLo) available, the council was unable to provide mandatory training on the requirements of GDPR in the lead up to its implementation. The GDPR e-learning module was only made mandatory in March 2019 and the completion rate has been low. In addition, there are no formal arrangements in place to monitor completion of this training.

[1] Heads of Service and above

The council has appointed appropriate officers to the key data protection roles of Senior Information Risk Owner, Caldicott Guardian and Data Protection Officer (DPO). The Audit and Governance Committee is provided with regular reports on information governance and also routinely considers the council's key corporate risks, one of which relates to information governance. Internal governance is principally centred on the Governance, Risk and Assurance Group (GRAG) and Council Management Team (CMT). Information governance is a standing agenda item at GRAG meetings and the DPO regularly attends CMT to provide information governance updates and to present on specific topics.

Overall Conclusions

The arrangements for managing risk were satisfactory with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made. Our overall opinion of the controls within the system at the time of the audit was that they provided Reasonable Assurance.

1 Policy and guidance

Issue/Control Weakness	Risk
The council does not have a data protection policy and sufficient guidance covering all activities that are required under the GDPR.	The council does not fulfil the requirements of the GDPR and is subject to censure from the ICO.

Findings

The council has not developed a data protection policy which sets out how it will comply with the requirements of data protection legislation. Article 24 of the GDPR requires that data controllers implement “appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with this Regulation”. One such measure is the implementation of "appropriate data protection policies”. It is good practice to make this available to members of the public so that they understand how they can expect the council to process their data and fulfil their rights under the GDPR. It is, however, recognised that the council has made information on rights available to the public as part of its corporate privacy notice. A draft Data Protection Policy Statement was presented to the Governance, Risk and Assurance Group at its 17 October 2018 meeting but it has not since been approved and launched.

In addition to the policy there is a requirement for accompanying procedures and performance standards for the activities that the council is obligated to perform under the GDPR to ensure that compliance is able to be achieved. As was reported at the 11 April 2018 Audit and Governance Committee meeting, the council has been developing a 'toolkit' approach to structuring its information governance policy and procedure framework. This will see the traditional policies amended or replaced with procedures and standards that are more accessible to staff. However, as at the time of the audit (April 2019), the toolkit had not been completed. Guidance is already provided to staff when they interact with the Freedom of Information, subject access and breach management processes but there is a lack of centrally available guidance on other requests made under other the rights of individuals, Data Protection Impact Assessments and on information sharing agreements.

Agreed Action 1.1

The toolkit will be finalised and approved. Once approved, the toolkit will be publicised internally and published on the intranet, with targeted awareness and training sessions delivered. The data protection policy statement will be made available on the council’s website.

Priority	2
Responsible Officer	Information Governance and Feedback Team Leader
Timescale	31 October 2019

2 Privacy information

Issue/Control Weakness	Risk
Sufficient privacy information may not be available to cover the specific processing activities carried out by service areas.	The council does not supply sufficient privacy information and fails to comply with the right to be informed under the GDPR.

Findings

The service area privacy notices available on the council's website were compared with the service areas recorded on the council's information asset register (IAR). Only just over a third (36%) of service areas represented in the IAR have a privacy notice on the council's website.

Some of what the council will have by way of privacy information is likely be in a format in which the service areas interact with the service user. This is reasonable and appropriate as the requirement of the right to be informed is to provide privacy information to individuals at the time personal data is collected from them. However, it is unlikely that this is the case for all service areas and teams for which a privacy notice is not available. No specific exercise has been undertaken by the council to match service area data processing to available privacy information and so assurances could not be obtained in this way.

On a risk basis, some of the most notable service areas for which a privacy notice is not available are Community Safety, Legal Services, Income Services, the Business Intelligence Hub and Licensing all of which will process special category data and possibly also criminal offence data.

Agreed Action 2.1

A programme of work will be developed, in conjunction with service areas and directorates, to identify gaps in the provision of privacy information for higher risk processing. Once all gaps have been identified, the Information Governance and Feedback Team will provide support to service areas in developing and publishing appropriate privacy information so that individuals' right to be informed is met.

Priority	2
Responsible Officer	Information Governance and Feedback Team Leader
Timescale	31 October 2019

3 Completeness of the information asset register

Issue/Control Weakness	Risk
The information asset register is incomplete.	The council has not fully defined its information assets and so processes data unlawfully.

Findings

A sample of 10 of the council's information assets were selected at random for review. It was found that information assets are recorded to varying levels of completion.

All information assets were missing at least some contextual detail as to the format, location, source and size of the asset. This information is not essential for ensuring lawful processing but should be recorded as it influences the type of controls and risk management required in order to safeguard the related data. Multiple assets recorded that a privacy notice was not available when, in fact, it was. This would suggest that these asset records are outdated. In other cases, a privacy notice was recorded as not being available when it should be. The majority of information asset records also did not specify a retention period. In addition, several information assets had not recorded the legal basis for processing and, where this had been recorded, inconsistencies were noted in the requirement for opt-in consent for processing and in the legislation quoted from which the lawful basis for processing is derived (i.e. from legislation other than the GDPR).

Agreed Action 3.1

Improvements and developments to the IAR application already identified will be formally requested from ICT so that they can be included in the ICT work programme. One such development will be enhanced reporting capability, the outputs from which will form part of the DPO's regular information governance update to CMT.

Priority	2
Responsible Officer	Information Governance and Feedback Team Leader
Timescale	31 October 2019

Agreed Action 3.2

A programme of work will be developed, in conjunction with service areas and directorates,

Priority	2

to identify gaps in information asset entries. Once all gaps have been identified, the Information Governance and Feedback Team will provide support to service areas in completing their information asset records and in ensuring that they are kept under regular review.	**Responsible Officer**	Information Governance and Feedback Team Leader
	Timescale	31 October 2019

4 GDPR variations to contracts

Issue/Control Weakness	Risk
It cannot be confirmed that the highest priority contracts have been varied so as to include the council's standard GDPR clause.	The council is not contractually protected from financial penalties imposed by the ICO for data breaches and so has to pay any resulting fine.

Findings

The council has created a new standard GDPR clause and data processing schedule for inclusion in all new contracts where the council is acting as the data controller and the contracting party as the data processor. In addition to the new clause and schedule, the Legal Services department has created template documents to be used to incorporate GDPR processing terms into existing contracts depending on the provision that is made for variations to these contracts.

In preparation for the GDPR, contract managers compiled spreadsheets containing details of the active contracts under their remit and whether or not these involved the processing of personal data. Legal Services then reviewed these spreadsheets and the original contracts in order to put the contracts into a priority order depending on the length of contract (any which were due to expire within a matter of months of the compliance exercise being commenced were considered lower priority), relationship between the council and the provider (any which were identified as being joint controller situations were again considered a lower priority) and the type of service being provided.

A total of 17 contracts were identified as high priority for variation. These contracts were compared with the variations that had been signed and returned to date as per section four of the Legal Services GDPR compliance document. This section is to be added to so that there is a record of the variations agreed and the method by which they were agreed. It was found that none of the 17 highest priority contracts identified in the priority lists featured in the list of varied contracts in section four. When the list at section four was cross-referenced back to the priority lists, it was found that only seven of the 22 contracts varied as per section four were recorded in the priority lists. Furthermore, all seven of the varied contracts were lower priority. Therefore, despite there appearing to be a robust process in place for considering all contracts and assessing, on a risk basis, the requirement for variations to be agreed, there is limited evidence that the highest priority contracts have been varied appropriately.

Agreed Action 4.1

Legal Services will investigate the status of the high priority contracts and will put arrangements in place to ensure that the council is adequately protected from any failure of its contractors to comply with the requirements of the GDPR.

Priority	2
Responsible Officer	Interim Assistant Director – Legal and Governance
Timescale	31 October 2019

5 Training

Issue/Control Weakness	Risk
Arrangements for ensuring completion of relevant data protection training are not fully effective.	Data is processed unlawfully as the requirements of the GDPR are not understood by all staff.

Findings

A number of issues were identified with the effectiveness of processes for ensuring completion of training on the GDPR. These are summarised as follows:

The 'GDPR: Data Protection Essentials' module on the MyLo training platform was first launched in July 2018 but did not become mandatory until it was re-launched at the beginning of March 2019. The instruction communicated to all staff was that the training should be completed by the end of April 2019. The latest available figure for the number of staff having completed the training was 701 at the end of March 2019 relative to an establishment of 2,573. This represents just over one quarter (27%) of the workforce. More staff will have completed the training in April but the council is clearly some way off achieving full completion. If a serious data breach was to occur and this was the responsibility of a member of staff who had not completed the training, this would harm the council's chances of defending its position with the ICO.

Discussions held with the Workforce Development Unit confirmed that there are no arrangements to provide the DPO with data on the completion status for the mandatory GDPR training. While it is the responsibility of the employee's line manager to ensure training is completed, the DPO is tasked with monitoring compliance with the GDPR and this necessarily includes training. Information on training completion should therefore be provided and reviewed so that the extent of compliance can be assessed and the necessary actions taken.

The induction process does include training and guidance on matters relating to information governance. However, it is not formally included as part of the induction checklist that is completed by the new starter and their line manager and is instead provided through the scheduled induction presentations. Depending on the commencement date for new starters, this could mean that they have been in the employment of the council for several weeks before they are made aware of their responsibilities in relation to data protection.

In the Information Governance and Complaints report presented to the Audit and Governance Committee on 26 July 2018, the DPO advised that targeted training would be provided to Information Asset Owners (IAOs) and Information Asset Administrators (IAAs). The DPO pursued this with the National Archives but was unable to secure the training with this provider. Guidance on roles and responsibilities for IAOs and IAAs has been made available to staff on the intranet since December 2018 but this has not been widely publicised and it is not a substitute for targeted training.

Agreed Action 5.1		
The 'Dojo: Local Government' information governance and cyber awareness eLearning solution will be rolled out to all staff as a mandatory training requirement.	**Priority**	2
	Responsible Officer	Information Governance and Feedback Team Leader
	Timescale	31 October 2019

Agreed Action 5.2		
The DPO will discuss with HR possible options to improve the induction process with respect to mandatory data protection training.	**Priority**	2
	Responsible Officer	Information Governance and Feedback Team Leader
	Timescale	31 October 2019

Agreed Action 5.3		
Targeted training for key information governance roles of SIRO, IAO and IAAs will be sourced and provided.	**Priority**	2
	Responsible Officer	Information Governance and Feedback Team Leader
	Timescale	31 October 2019

Agreed Action 5.4

Arrangements will be put in place between the Workforce Development Unit and the Information Governance and Feedback Team to receive regular reports on completion of mandatory data protection training. Data on training completion rates will form part of the DPO's regular information governance update to GRAG, CMT and DMTs.

Priority	2
Responsible Officer	Information Governance and Feedback Team Leader
Timescale	31 October 2019

6 Data security incident reporting arrangements

Issue/Control Weakness	Risk
There is a lack of management information on data security incidents.	Area of non-compliance or weakness are not identified and addressed, increasing the likelihood of further incidents and possible censure from the ICO.

Findings

The 2014-15 audit of Information Security found that quarterly summaries of information security incidents were produced and reported to Corporate Information Governance Group (CIGG) meetings (this group is no longer in existence and has been replaced with the Governance, Risk and Assurance Group (GRAG)). It was observed that the reports summarised each incident individually, including the cause and a brief description of every incident reported but other aspects of compliance with the information security incident policy and procedure, such as the timeliness with which incidents are reported and whether appropriate action has been taken in response to the incident, were not reported on. The audit agreed an action that a system would be developed which would provide for oversight and monitoring of information security incidents through CIGG, Council Management Team (CMT) and Directorate Management Teams (DMTs).

While information governance is a standing item at GRAG and it is routinely reported on at CMT, this does not include the information described above in respect of data security incidents. The DPO has advised that thematic information on data security incidents is reported verbally to GRAG and to CMT but there is limited evidence to support this. In any case, presentation of the information verbally does not allow members of GRAG or CMT to challenge interpretation of the data and to get their own assurances as to the extent of compliance with the breach management policy or to identify where action is needed to address weaknesses.

Agreed Action 6.1

Themes arising from reported and investigated personal data breaches will be reported to GRAG, CMT and DMTs and to Audit and Governance Committee as part of the DPO's regular information governance update.

Priority	3
Responsible Officer	Information Governance and Feedback Team Leader
Timescale	31 October 2019

Audit Opinions and Priorities for Actions

Audit Opinions
Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit. Our overall audit opinion is based on 5 grades of opinion, as set out below.

Opinion	Assessment of internal control
High Assurance	Overall, very good management of risk. An effective control environment appears to be in operation.
Substantial Assurance	Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
Reasonable Assurance	Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
Limited Assurance	Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No Assurance	Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

Priorities for Actions	
Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.