Report to:

GDPR Project Review

2 October 2018

Contents

Status of our reports

This report ("Report") was prepared on the basis of the limitations set out in Appendix 6 by Mazars LLP at the request of City of London Corporation (CoL) 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 work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Mazars 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.

Executive Summary

Background

The City of London Corporation (CoL) provides services such as environment protection, housing, council tax, children and adult social care, to a residential population of approximately 8,000 people. There are however over 400,000 people that commute into the City every day for work and over 10 million visit as tourists every year.

At the request of the CoL, Mazars LLP has undertaken a review of their GDPR Project Plan for the introduction of, and compliance with, the General Data Protection Regulation (GDPR) legislation.

Adopted in April 2016 by the European Union, the GDPR came into effect on 25th May 2018. The legislation is intended to strengthen data protection rights for individuals within the EU.

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.

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.

Leading up to May 2018, the CoL has engaged with Mazars to undertake a review of their GDPR Project Plan and a high level overview of the CoL's data privacy governance, to assess the current preparations for compliance.

The ICO's 12 steps guidance includes processes that should already be in place (to comply with the Data Protection Act 1998):

1. **Awareness**: You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.
2. **Information you hold**: You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.
3. **Communicating privacy information**: You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4. **Individuals' rights**: You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
5. **Subject access requests**: You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.
6. **Lawful basis for processing personal data**: You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.
7. **Consent**: You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.
8. **Children**: You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.
9. **Data breaches**: You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.
10. **Data Protection by Design and Data Protection Impact Assessments**: You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party and work out how and when to implement them in your organisation.
11. **Data Protection Officers**: You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.
12. **International**: If your organisation operates in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

Purpose of Review

The objective of the review is to provide an independent, objective opinion on the CoL's GDPR Project Plan and data privacy governance taking into account the implementation in progress.

Scope of Review

- Assessment of plans in place to address GDPR, including identifying responsibility for ensuring that all areas are covered and no gaps are left leading up to the implementation of the new rules;
- Overview of the main areas of risk in relation to the new GDPR regulation; and
- Assessment of general awareness amongst staff in relation to the new regulation.

The Terms of Reference for this review are included in Appendix 5.

Key Findings

Priority	Number of recommendations
HIGH	2
MEDIUM	0
LOW	5
TOTAL	7

Summary of the issues identified as a result of our work

The CoL has achieved material compliance with GDPR, as they have all the necessary measures in place and are in progress of becoming fully compliant (please see 'Good Practices' section below), once all the below points have been fulfilled.

- The review of third party contracts has not been fully completed but there has been good progress to address these sufficiently i.e. contractual clauses for data sharing;
- A final retention policy has not been implemented, although this is currently under review. Furthermore, a formal review of all data stored on computer network drives is required, with the help of proposed diagnostic tools;
- The GDPR Project team and the Access to Information Network (AIN) representatives (reps) have worked and coordinated successfully on implementations tasks; however, the going use of the AIN reps should be regularly reviewed to confirm that their continued use meets the expected requirements;
- A mini gap analysis and follow-up audit is beneficial to ensure the tasks are completed and identify any remaining aspects of the GDPR implementation;
- There is ongoing 'Business As Usual' support by the Governance team to continue with GDPR compliance, alongside engagement with the AIN reps who monitor and support departments. The GDPR e-learning course suggests engagement; however, the remaining 6% out of the 94% completion should be identified in order to establish if they are active staff or not;
- Additional resourcing may be needed to embed compliance more actively in some departments, this could be utilised from the GDPR Project team.

Full compliance can be achieved within the organisation once all the above points have been completely accomplished. In particular the review of all data and successfully updating all third party contracts.

Within the overall findings, two 'high' and 5 'low' recommendations were identified during the course of the review. The rating definitions are outlined in Appendix 4.

Good Practices Identified

Areas of good practice / compliance identified during the review

During the course of this review, a number of good practices were identified, as follows:

- A phase two project plan is in place, which includes:
  - Designing a structured job role for the AIN reps;
  - Updating all third party contracts;
  - Follow-up training sessions, communications and reporting;
  - A mini gap-analysis and a follow-up audits across departments;
  - A final retention policy and diagnostic software (sniffing tool) to be enforced; and
  - Investigation tools and meta compliance tools to assess compliance.
- The GDPR project will continue to embed compliance within phase 2 of the implementation and address all key issues, which will run until the 31 December 2018. The Comptroller and City Solicitor was appointed as the Data Protection Officer (DPO) in September 2017. The DPO is of a legal background and is aware of the importance of GDPR compliance. The DPO has good support from senior staff members.
- The training plan indicates that 94% of staff have completed the training. They are keen to get this figure up to the full 100% and identify who the remaining 8% are against active staff.
- A final retention policy is being considered in order to build a formal review of data, which will be come into force in phase two of the implementation.
- There are AIN's reps within the organisation who are responsible for GDPR implementation tasks in their respective departments. They coordinate with the GDPR Project team to support and encourage compliance throughout departments.
- Since our initial review CoL has demonstrated substantial progress on key areas by taking into account our recommendations, particularly in relation to the size of the organisation.

Findings and Recommendations

Ref	Finding	Recommendation	Management responses	Priority
1	**Reviewing third party contracts**			
	The reviewing of existing third party contracts has not been fully completed in compliance with the GDPR, particularly contracts with suppliers to ensure data sharing is consistently compliant. It is, however, noted that good progress is being made on the review of third party contracts, in particular updating contractual clauses and data sharing agreements which are yet to be finalised. These contracts must be amended before transferring data to third parties. Moreover, an assessment of contracts that are high risk also need to be completed, by identifying where CoL are controllers or processors, where applicable and taking into account the relevant lawful basis for processing.	The review of the third party contracts requires immediate action if data is transferred between third parties, particularly those that are of high risk where CoL is the data controller and those with suppliers. However, we are aware this is a core focus within phase two of the implementation and it should be flagged as vital to continue processing compliantly. Distinction between where COL is a data controller and data processor is also necessary to determine the responsibility.	Departments have been collating a standard format Contracts Register for live contracts with third parties who process personal data on behalf of the City of London Corporation as a data controller. This has been a time-consuming exercise and progress has been made with 66% of departments in scope submitting returns. A progress report was sent to Chief Officers on 16.10.18 and will be further reported in the GDPR progress report to IT-sub committee on 02.11.2018. When all returns are received, a Corporate Register of contractor GDPR compliance will be created exceptions and non-responses will be reported to Chief Officers for rectification. Responsibility: Departmental Managers supported by departmental AIN reps and the C&CS Information Compliance Team Target Implementation Date: 31 December 2018	**High**

Ref	Finding	Recommendation	Management responses	Priority
2	**Retention policy**			
	A final records retention schedule has not been implemented, which is particularly concerning considering the vast amount of information stored. Although there is a generic records retention policy that forms the basis of the final version this has not yet come into force; it is noted at the time of audit, however, that progress has been made in terms of departments reviewing their own retention schedules as part of the final one. In addition to this, a formal review of the data stored both physically and electronically is necessary to identify what information needs to be retained or deleted. The concerns are around unstructured data, and the 'W Drive' is an example of a server that has a vast amount of information. The Information Management team is encouraged to review and manage the data stored on network drive. Based on the interview with the Deputy IT Director, we understand that this can be achieved using diagnostic software known as 'Sniffing Tools'. The IS team is also investigating tools to identify and manage all unstructured data to ensure compliance with GDPR. Although this is a grey area that has not yet reached full compliance there are good measures in place to satisfy this going forward.	CoL should ensure that the final retention schedule is put into place rapidly, in order to ensure all staff are aware of how long they should potentially keep their physical and electronic data for. A data cleanse or destruction review is essential in managing data throughout the organisation, in order not to keep information 'for longer than is necessary', particularly if the purposes it was collected for has been completed. This will be deemed unnecessary as there is unlikely to be a lawful basis for retention. Ensuring that data is either erased or anonymised when you no long require it will reduce the risk of it becoming irrelevant, excessive, inaccurate or out of date. This will help comply with the data minimisation and accuracy principles under the GDPR. This should be accessed immediately and followed up on an annual basis, with help from the 'sniffing tool' and any other investigating tools that will assist with this.	**a) Records Retention** Good progress has been made on departmental records retention schedules but 8 departments are yet to submit schedules In addition to local schedules, there is the 83 page CoL Model Retention Schedule which has also been updated. For info. there is a draft Records Management policy from 2015 which will be revised and re-issued as part of the corporate Information Management Review. Responsibility: Departmental Managers supported by departmental AIN reps and the C&CS Information Compliance Team Target Implementation Date: 31 December 2018 **b) Data Storage / Discovery** This remains as a red risk on the GDPR plan. Currently awaiting costs from 4 potential suppliers. This should be two separate findings – Records Retention Schedules and Data Discovery & Retention. We have some control over Records Retention but Data Discovery & Retention is largely dependant on a 3rd party service provider. They are separate items on the project plan. Responsibility: IS Department Target Implementation Date: 31.03.2019	**High**

Ref	Finding	Recommendation	Management responses	Priority
3	**Review of GDPR programme governance arrangements**			
	The GDPR project team and AIN reps are responsible for the coordination of implementation tasks throughout the organisation. The governance structure has been regarded as efficient as support has been provided at department level; however, this needs to be finalised in terms of the structured job role for the AIN reps and having the appropriate tools in place to assess and monitor compliance. Moreover, the use of AIN reps should be reviewed to ensure that the process meets the City's success criteria.	Using tools such as Balanced Scorecards should provide granular updates of completion of tasks. Going forward it is beneficial that the GDPR project team will produce reports to keep track of the progress and communicate this with the AIN reps, to monitor progress or take further action where required.	A Self-Audit Compliance Monitor has been developed with input from some AIN Reps and business users. This has been issued to departments for completion in October 2018. Returns will be analysed high risks will be identified and AIN reps advised accordingly to improve compliance standards. AIN reps will provide the base compliance data, the responsibility for managing compliance lies with departmental management teams. A review of the AIN role in the wider context of Information Management will be conducted as part of the IM Review. Responsibility: Departmental Managers supported by departmental AIN reps and the C&CS Information Compliance Team Target Implementation Date: 31.12.2018	**Low**

Ref	Finding	Recommendation	Management responses	Priority
4	**Mini-gap analysis and a follow-up audit**			
	There is no further gap analysis or follow-up audit to identify any issues going forward, for the remaining aspects of the GDPR implementation.	A mini-gap analysis and follow-up audit for each department should be undertaken as it will ensure all outstanding tasks have been addressed, particularly due to the size of the organisation. This should be documented on a department level to see where improvements can be made. It will incorporate a direction going forward for phase two of the implementation. We are aware that the above points will be a focus in phase 2 of the GDPR implementation.	A Self-Audit Compliance Monitor has been developed with input from some AIN Reps and business users. This has been issued to departments for completion in October 2018. Returns will be analysed high risks will be identified and AIN reps advised accordingly to improve compliance standards. Responsibility: Departmental Managers supported by departmental AIN reps and the C&CS Information Compliance Team Target Implementation Date: 31 December 2018	Low

Ref	Finding	Recommendation	Management responses	Priority
5	**GDPR is not seen as an ongoing 'Business as Usual' (BAU) responsibility**			
	Based on staff interviews, there is a concern that individuals in the organisation at all levels do not see GDPR as an ongoing BAU responsibility and that there may not be enough change at an individual level. However, this finding is based only on a small sample of representatives and there has been an ongoing BAU by the Governance team for many years under the previous Data Protection legislation to try and incorporate compliance and will continue throughout the GDPR.	The Governance team, Project team and the AIN reps should continue to communicate with staff on the importance of GDPR under BAU practices. Staff should be regularly informed of their accountability and responsibility when collecting and processing data under the GDPR. A GDPR compliance checklist and Q&A sessions will endure engagement and remain consistent with compliance measures.	The Self-Audit Monitor will help identify areas which need to be managed. Also, the key GDPR polices will be re-issued and tracked by meta-compliance. The DPO has started quarterly AIN Forums to share knowledge and information on GDPR compliance issues and news. This will be supported by more general GDPR comms. Annual GDPR refresher e-learning is scheduled. Further specialist GDPR training will be delivered in response to feedback from AIN reps and where specific risks of non-compliance are identified by the Information Compliance Team. Responsibility: Departmental Managers supported by departmental AIN reps and the C&CS Information Compliance Team Target Implementation Date: 31 December 2018	**Low**

Ref	Finding	Recommendation	Management responses	Priority
6	**GDPR e-learning**			
	A GDPR e-learning course was sent out on 24 April and was expected to be completed by 18 May. The initial completion rate reported was 63%. The most recent completion on the GDPR e-learning course increased to 94%, which suggests there has been more engagement around GDPR.	The CoL should identify whether they are active staff that may have potentially affected the results. CoL should also devise a communication strategy or procedure to address the remaining staff whom are yet to complete the GDPR e-learning course. We also suggest that CoL should ensure that GDPR e-learning is integrated with the induction training of all new joiners.	E-learning compliance levels were analysed by departments and reported to Chief Officers on 16.10.2018 and will be further reported to IT sub-committee on 02.11.2018. Annual GDPR refresher e-learning is scheduled. Responsibility: Departmental Managers supported by departmental AIN reps and the C&CS Information Compliance Team Target Implementation Date: 31.03.2019 ongoing thereafter	Low

Ref	Finding	Recommendation	Management responses	Priority
7	**Additional resources**			
	Based on staff interviews, there were concerns that additional resourcing could be needed to complete certain tasks, such as reviewing third party contracts. As discussed in the closing meeting, the CoL believe they already have the correct resources within the organisation and do not believe additional resourcing will make a big impact.	If there are difficulties meeting the December deadline then additional resources either internally or externally should be considered. Further resources may be necessary, particularly for the Compliance and IS teams. This could be utilised from the GDPR Project team to assist in to embedding GDPR compliance throughout all CoL departments.	The compliance team is correctly resourced to deliver of the CoLC GDPR project phase 2. Ownership of GDPR should transition to BAU by December the Compliance Team will then manage ongoing GDPR governance, undertake follow-up audits, deliver GDPR refresher training, monitor and analyse data breaches and deliver communications and networking. Responsibility: Departmental Managers supported by departmental AIN reps and the C&CS Information Compliance Team Target Implementation Date: 31.12.2019 ongoing thereafter	Low

Appendix 1 – Glossary

TERM	DEFINITION
DATA	Is: (a) Information which is recorded to be processed by equipment which has been instructed for that purpose; (b) recorded as part of or with the intent of forming part of a relevant filing system; (c) recorded information held by a public authority; or (d) forms part of an accessible record (health, educational, etc.).
PERSONAL DATA	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
SENSITIVE DATA	Personal data of the subject consisting of the following information: (a) ethnic origin; (b) political opinions; (c) religious or similar beliefs; (d) membership of trade union(s); (e) physical and mental health; (f) sexual life; (g) commission or alleged commission of any offences; or (h) any court proceedings pertaining to (g).
PROCESSING	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
DATA SUBJECT	To whom the personal data pertains.
DATA CONTROLLER	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
DATA PROCESSOR	Any person other than an employee of the Data Controller who processes data on the Data Controller's behalf.
INACCURATE DATA	Data which is incorrect or factually misleading.
RECIPIENT	A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
THIRD PARTY	A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Appendix 2 – Documents Reviewed

List of documents reviewed as part of the engagement

- GDPR Project Plan;
- List of people in the GDPR project board;
- GDPR project board minutes;
- Contact details and job description of the Data Protection Officer;
- Records of processing activities (information register or data mapping);
- Data transfers register;
- Privacy Notices;
- Templates of terms and conditions of employment;
- Employee handbook;
- Employee Data protection policy;
- Data retention policy;
- Data breach policy;
- Data breach notification templates;
- Information security policy;
- Data protection and data breach training material to employees;
- Standard data sharing agreement template used with third parties;
- Evidence of marketing changes regarding consent;
- Back-up policy;
- Vulnerable scanning policy;
- Use of IT posters; and
- Audit and Risk Management Committee papers.

Appendix 3 – Staff interviewed

Name	Title
Daniel Mckee	Comptrollers
Jimmy Maravala	Community and Children's Services
Terry Morris	HR
Carol Simpson	HR
Matt Gosden	IS
Colin Tharby	IS

Mazars LLP appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and cooperation.

Appendix 4 – Rating Definitions

Recommendation significance

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

Priority Level	Definition
HIGH	Major issues for the attention of senior management. Such issue must imperatively be addressed before the 25th May 2018 as it can lead to an important fine or serious reputational damage.
MEDIUM	Important issues to be addressed by management in their areas of responsibility. Such issue must be included in the GDPR compliance project plan to be implemented as soon as possible, preferably before the 25th May 2018.
LOW	Minor issues that, although not essential, should be included in the GDPR compliance project plan as a matter of good practice and be implemented by the end of the year 2018.

The risks in this report have been assessed by considering the two levels of fines introduced in the GDPR, as shown in the table on the next pages.

Additional consideration is given when assessing the risks when processing activities involve special categories of data, as defined in Article 9 of the GDPR, or data relating to criminal conviction and offences, as defined in Article 10 of the GDPR. Such personal data must be processed with particular attention under the GDPR, especially in respect of data subjects' rights, legal basis for processing, international transfers, and implementation of proportionate security measures. The ICO's case law and the Article 29 Group's guidelines have also been taken into consideration to assess the risks.

Maximum administrative fines for non-compliance with GDPR Articles below and to which entity apply:	Up to €20m or 4% of global annual turnover, whichever is higher	Up to €10m or 2% of global annual turnover, whichever is higher
Art. 5 - Principles relating to processing of personal data	Controller	
Art. 6 - Lawfulness of processing	Controller	
Art. 7 - Conditions for consent	Controller	
Art. 8 - Conditions applicable to child's consent in relation to information society services		Controller
Art. 12 to 22 – Rights of data subjects	Controller	
Art. 25 - Data protection by design and by default		Controller
Art. 26 – Agreements between joint controllers		Controller
Art. 27 – Designation of representatives of controllers or processors not established in the Union		Controller and Processor
Art. 28 – Controller engagement of processors		Controller
Art. 29 – Processors acting only under the consent and instructions of the controller		Processor

Maximum administrative fines for non-compliance with GDPR Articles below and to which entity apply:	Up to €20m or 4% of global annual turnover, whichever is higher	Up to €10m or 2% of global annual turnover, whichever is higher
Art. 30 – Written records of processing activities		Controller and Processor
Art. 31 - Cooperation with the supervisory authority		Controller and Processor
Art. 32 - Security of processing (technical and organisational measures)		Controller and Processor
Art. 33 – Data breach reporting		Controller and Processor
Art. 34 – Data breach communication		Controller
Art. 35 – Conduct data protection impact assessments		Controller
Art. 36 – Consultation supervisory prior to processing after data protection impact assessment indicates high risk		Controller
Art. 37-38-39 – Appointment Data Protection Officer		Controller and Processor
Art. 44 to 49 - Transfers of personal data to third countries or international organisations	Controller and Processor	
Art 58 – Failure to comply with an order or with an investigation imposed by supervisory authorities	Controller and Processor	

Appendix 5 – Objectives and Scope

Background:

The new General Data Protection Regulation (GDPR) comes into force on 25 May 2018. Through GDPR, the European Commission seeks to strengthen and unify data protection for natural persons situated within the EU. An early, high level assessment will be made of CoL's plans and readiness to address the new requirements, to continue being compliant after 25 May 2018.

Audit objective and scope:

The primary purpose of this review is to provide an independent, objective assessment of CoL compliance with the GDPR requirements, and status of project plans CoL has in place.

Scope:

The primary purpose of this review is to provide an independent, objective assessment of CoL's readiness for the forthcoming GDPR requirements, and status of project plans CoL has in place.

This review will focus on the following areas:

- An assessment of the plans in place to meet with GDPR which came into force from May 2018. The audit will identify appropriate responsibility and plans to ensure that all areas are covered and no gaps are left;
- To review progress of CoL's GDPR risk assessment; and
- An assessment of general awareness amongst CoL's staff and Senior Management in relation to the new regulation.

We will bring to the attention of management any significant matters relating to these or other areas that come to our attention during the course of the review.

Approach

Our approach to the review will be as follows:

- Review progress of the work towards GDPR compliance via documentation review and discussions with appropriate personnel;
- Validate the risks identified and assess the project plans in place;
- Identify gaps for the areas under review; and
- Hold closing meetings with relevant key personnel to discuss audit findings and recommendations.

Type of Report:

A final report will be provided which will entail an executive summary of the key findings.

The report will also include detailed issues with agreed action plans assigned to the relevant individuals and agreed timeframes.

All issues raised in the final reports are monitored and issues falling overdue will be escalated to the Audit Committee.

Date of fieldwork:

It is proposed that fieldwork will start on 7 May 2018 and resource requirements are estimated at 4 days with 1 day to write and review the report. Total resources are therefore estimated to be 5 days.

Key contacts:

Engagement Director	Mark Towler	mark.towler@mazars.co.uk
Senior Manager, Data Privacy	Vincent Rezzouk-Hammachi	vincent.rezzouk@mazars.co.uk
Data Privacy Consultant	Safeena Tariq	safeena.tariq@mazars.co.uk
Data Privacy Consultant	Liam McKenzie	liam.mckenzie@mazars.co.uk
Data Privacy Consultant	Paul Seseri	paul.seseri@mazars.co.uk

Deliverable	Dates
Fieldwork start	07/05/2018
Fieldwork completion	25/05/2018
Exit meeting	31/05/2018
Draft report issued	28/06/2018
Final report issued	TBC

Appendix 6 – Statement of Responsibility

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.

Mazars LLP accepts no duty of care to any person (except to the CoL under the relevant terms of the engagement) for the preparation of the report.

Accordingly, regardless of the form of action, whether in contract, tort or otherwise, and to the extent permitted by applicable law, Mazars LLP accepts no liability of any kind and disclaims all responsibility for the consequences of any person (other than the CoL on the above basis) acting or refraining to act in reliance on the report or for any decisions made or not made which are based upon such report, regardless of whether or not the CoL has consented to the disclosure of this report.