MOPAC | MAYOR OF LONDON
OFFICE FOR POLICING AND CRIME

Directorate of Audit, Risk and Assurance
Internal Auditors to MOPAC

Risk and Assurance Review
January 2019

MOPAC General Data Protection Regulation (GDPR) Governance Framework

Contents

Executive Summary

1. Background

1.1 The Mayor's Office for Police and Crime (MOPAC) aims to ensure it has an effective framework in place to support the implementation of the changes in key data protection legislation under the new General Data Protection Regulation (GDPR). This review provides assurance on the measures taken to date and those planned to ensure compliance with the legislation. The full terms of reference are attached at the end of the report.

1.2 The GDPR was approved by the EU Parliament on 14 April 2016 and came into effect in May 2018 alongside the Data Protection Act 2018. GDPR aims to ensure businesses and organisations collect, process and delete personal data in a fair and secure manner to protect data subjects and introduce new rights to give individuals better control over their personal data.

1.3 The GDPR has defined data controllers and processors to identify roles, responsibilities and legal obligations. This impacts on organisations such as MOPAC who process personal data, engage with large numbers of people, both the public and stakeholders and have also outsourced functions such as payroll, occupational health, legal advice, benefits, healthcare screening, employee support and training provision. Non-compliance with GDPR could lead to significant fines and reputational damage to both data 'controllers' and 'processors'

1.4 MOPAC's key challenge is to ensure that existing personal data processing activities are reviewed and revised to meet the GDPR data handling requirements and meet the increased public awareness in handling their personal data while maintaining business processes to meet the aims and objectives of the Police and Crime Plan.

1.5 MOPAC has developed a GDPR Implementation Action Plan. This is used to govern the implementation of the required GDPR regulatory changes and incorporate them in MOPAC policies and procedures to enable compliance and continually assess progress made.

2. Audit Assurance

Adequate

The control framework is adequate and controls to mitigate key risks are generally operating effectively, although a number of controls need to improve to ensure business objectives are met.

3. Areas of Effective Control

3.1 There is a comprehensive project plan in place for GDPR implementation to ensure that MOPAC complies with the key GDPR changes. This was presented to the Governance and Risk Working Group (GRWG) on 16 January 2018 and is used to monitor progress. GDPR is reported to the Senior Information Risk Officer (SIRO) through the GRWG on a monthly basis. The project plan has continued to be developed to ensure GDPR compliance is incorporated into MOPAC policies and procedures, staff training, contract and grant management and information security arrangements as appropriate.

3.2 GDPR is included in the MOPAC corporate risk register under information management. The SIRO is the identified risk owner and the GDPR Project Manager is the risk lead and action owner. The risk register was last updated in November 2018 and information management has been rated as an amber risk. Key mitigations have been agreed and are reflected in the GDPR project and action plan.

3.3 Roles and responsibilities for GDPR have been clearly established. All MOPAC staff are responsible for implementing information governance good practice on a day to day basis through compliance with approved policies and procedures. The Senior Management Team (SMT) oversees and monitors information governance issues as part of the GRWG. The MOPAC Director of Strategy is the SIRO and the Head of Strategy and Corporate Planning is the Data Protection Officer (DPO), responsible for managing and reporting on compliance with the GDPR and information governance. In addition, MOPAC appointed a GDPR project manager who has been responsible for developing and implementing the GDPR governance framework.

3.4 The GRWG serves as the GDPR Project Board and act as a reference group for policy review. The group also monitors progress against the GDPR project plan and any significant issues are reported via the DPO and GDPR Project Manager. The GRWG terms of reference includes the responsibility to gain assurance that there are robust processes in place within MOPAC for information governance. The MOPAC SMT are also briefed on progress with the latest update report provided and discussed on the 5 December 2018.

3.5 The GDPR Project Manager has provided MOPAC staff with internal communications, guidance and training on GDPR. All members of staff participated in a 'three peaks challenge', which included clearing paperwork, clearing personal drives and emails, clearing shared drives and Sharepoint. Regular updates on GDPR are provided via the weekly bird table and all staff emails.

3.6 MOPAC staff have been required to attend mandatory GDPR training to ensure they understand their responsibilities to deliver GDPR compliance. All MOPAC staff have received the training with HR maintaining a list of all those attending. GDPR has also been included as part of the induction process for new staff.

Executive Summary

3.7 Now that all MOPAC staff have received their mandatory GDPR training MOPAC will be introducing annual mandatory training for all staff on GDPR compliance. This will be implemented via a GDPR E-learning package.

3.8 The MOPAC staff privacy notice has been updated, emailed to all staff and is available on the MOPAC GDPR intranet page. The privacy notice outlines the data MOPAC holds, the reasons for holding the data, the legal basis for using the data and rights of staff see any personal information MOPAC holds. The notice also outlines those third parties who process data on MOPAC's behalf.

3.9 MOPAC has updated the external privacy notice, which outlines what to expect when the MOPAC collects personal information. The privacy notice can be accessed via the MOPAC internet site.

3.10 Policies and procedures have been developed to accommodate GDPR requirements including information governance, handling of personal data via the staff privacy notice and privacy policy are published on the MOPAC website. A records management policy, data protection policy, retention and review and disposal policy are also in place. Guidance is available on SharePoint for MOPAC staff when dealing with Correspondence and GDPR compliance.

3.11 A data breach process is in place on personal data incidents and breaches and is available to staff on Sharepoint. The process outlines the steps to take when dealing with a potential personal data breach and the process to follow in deciding if the breach is notifiable. MOPAC staff have also been trained on what to do if they suspect a breach. The process also identifies the key MOPAC contacts.

3.12 MOPAC has started to include GDPR in its decision-making process for all new programmes and projects that use personally identifiable information for members of the public and any ongoing programmes and projects that represent risks to data subjects. The MOPAC Data Protection Impact Assessments (DPIAs) templates have been developed for MOPAC and suppliers in line with the requirements of the ICO DPIA guidelines. At present there are 19 DPIAs of which four have been completed, nine in draft stage, three are in the process of being drafted and three have not been completed. All DPIAs are required to be signed off by the DPO. There is on-going advice and support in place for staff on specific DPIA advice and support delivered to ensure DPIA sign off.

3.13 Decision making templates for the Deputy Major for Policing and Crime, Chief Executive Officer and Directors have all been updated to ensure GDPR compliance issues are covered in the body of each report and the GDPR Project Manager/Data Protection Officer are consulted on the GDPR issues within the report. All reports need to state that GDPR or data privacy issues have been considered and where necessary are applicable.

3.14 All CJC providers have been contacted to notify them of MOPAC's GDPR compliance requirements. In total 46 providers have been contacted of which 21 have been read, 1 was undelivered and 1 declined without reading. This will be followed up.

3.15 GDPR compliance text has been established for MOPAC contracts and grants. All MOPAC contracts and grants are required to state that nothing within the contract or grant relieves the processor of its own direct responsibilities and liabilities under the GDPR and reflects any indemnity that has been agreed. Responsibilities for GDPR compliance have been established for contracts and grants with providers where MOPAC is the commissioner and the provider is the controller, MOPAC and the provider are joint controllers and where MOPAC is the controller and the provider is the processor**.**

3.16 The MOPAC contracts register has been reviewed to identify where MOPAC and the supplier are the commissioner and the data controller. The GDPR Project Manager drafted a letter outlining the new GDPR regulations which suppliers should be adhering to and the relationship in terms of roles such as data controller and commissioner. A delegated officer will sign and return the letter to the contracts team prior to issue. The deadline to send out letters to suppliers is January 2019.

3.17 The SIRO and GDPR Project Manager meet the Information Commissioners Officer (ICO) quarterly to discuss Met compliance issues and have generally received positive feedback.

4. Key Risk Issues for Management Action

4.1 There is a need to embed GDPR requirements into the project and programme initiation process to ensure on-going GDPR compliance. There is also a need to ensure that resources are available to continue the development of the GDPR governance framework and maintain the processes in place to allow MOPAC to demonstrate compliance with GDPR.

4.2 A staff checklist for GDPR compliance has been introduced. All MOPAC staff were required to complete and sign the checklist, have it counter signed by their line manager and return it to MOPAC HR by 31 August. Eighty-nine staff have returned the GDPR checklists and 51 staff have yet to return the checklist. MOPAC HR is chasing the GDPR checklists and will be sending lists to line managers regarding returns which have not been received. Until this process is completed it will not be possible for MOPAC to provide assurance that it has documented the personal data held, where it came from, who it is shared with and what is done with it.

4.3 The GDPR states that organisations such as MOPAC who have fewer than 250 employees are not required to maintain a record of processing activities under its responsibility, unless “the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences”. MOPAC teams are in the process of reviewing and cleansing the data they hold and will need to determine whether the data held requires the maintenance of an Information Asset Register. Evidence and Insight have been identified as holding data, which will require an Information Asset Register and have started the process of producing the

register. The Information Asset Register is an important management tool for identifying data assets and to improve the understanding of MOPAC's business and information needs, spot opportunities for more efficient data handling and assign clearer data ownership. Failure to use the Information Asset Register when required as a management tool to maintain, update and review personal information could result in non-compliance with GDPR.

4.4 The GDPR project plan covers the ICO checklist for controllers and updates are regularly provided to the GRWG with RAG ratings for each task, however, it does not include target dates for completion of tasks and a number remain outstanding. The majority of outstanding tasks are related to creating a process to maintain records of processing activities as part of Information Asset Register. The lack of target dates may result in key issues not being promptly escalated and addressed by senior management.

Key Findings and Agreed Action(s)

1. GDPR Compliance Process - Medium Priority

Finding	Risk	Agreed Actions
There is a is a need to embed GDPR requirements into the project and programme initiation process to ensure on-going GDPR compliance. There is also a need to ensure that resources are available to continue the development of the GDPR governance framework and maintain the processes in place to allow MOPAC to demonstrate compliance with GDPR.	GDPR compliance is not fully supported and embedded in all key processes leading to non-compliance and/or a data breach.	i) GDPR requirements will be embedded in the project and programme initiation process and monitored for compliance throughout the project/programme. ii) Resources to support GDPR will be subject to regular management review and action taken as appropriate.
		Responsibility: Head of Governance and Risk
		Deadline: June 2019

2. Staff Checklist for Compliance - Medium Priority

Finding	Risk	Agreed Action
A staff checklist for the GDPR compliance has been introduced. All MOPAC staff were required to complete and sign the checklist, have it counter signed by their line manager and return it to MOPAC HR by 31 August. Eighty-nine staff have returned the GDPR checklists and 51 staff have yet to return the checklist. MOPAC HR is chasing the GDPR checklists and will be sending lists to line managers regarding returns which have not been received. Until this process is completed it will not be possible for MOPAC to ensure that it has documented the personal data held, where it came from, who it is shared with and what is done with it.	MOPAC staff are not complying with GDPR. Personally identifiable information is not removed from personal and shared drives in a timely manner leading to unnecessary data breaches, penalties and reputational damage.	All staff are required to complete their staff checklist and non-compliance will be reported to the Governance and Risk Working Group for further action.
		Responsibility: MOPAC HR and GDPR Project Manager
		Deadline: March 2019

3. Information Asset Register - Medium Priority

Finding	Risk	Agreed Actions
The GDPR states that organisations such as MOPAC who have fewer than 250 employees are not required to maintain a record of processing activities under its responsibility, unless "the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences". Teams within MOPAC are in the process of reviewing and cleansing the data they hold and will need to determine whether the data held requires the maintenance of an Information Asset Register. Evidence and Insight have already been identified as holding data which will require an Information Asset Register and have started the process of producing the register. The Information Asset Register is an important management tool for identifying data assets and to improve the understanding of MOPAC's business and information needs, spot opportunities for more efficient data handling and assign clearer data ownership.	Failure to use the Information Asset Register when required as a management tool to maintain, update and review personal information could result in non-compliance with GDPR.	i) MOPAC SLT members will review their processing of data to determine whether they are required to maintain an Information Asset Register under GDPR. SLT members will provide an assurance as to the results of their review. ii) Where necessary MOPAC teams will be required to maintain an Information Asset Register and review it on a regular basis and notify the DPO of the results of the review. Evidence and Insight have already begun the process of developing their Information Asset Register.
		Responsibility: Head of Governance and Risk
		Deadline: June 2019

4. GDPR Project Plan Implementation - Medium Priority

Finding	Risk	Agreed Action
The GDPR project plan covers the ICO checklist for controllers and updates are regularly provided to the GRWG with RAG ratings for each task, however, it does not include target dates for completion of tasks and a number remain outstanding. The majority of outstanding tasks are related to creating a process to maintain records of processing activities as part of Information Asset Register. The lack of target dates may result in key issues not being promptly escalated and addressed by senior management.	Actions agreed to ensure full compliance with Data Protection Legislation are not taken and non-compliance occurs.	The project plan will be amended to show target dates for completion, which will be monitored by the GRWG and action taken to address any areas that are not making adequate progress.
		Responsibility: GDPR Project Manager
		Deadline: January 2019

Business Objective

To ensure that the Mayor's Office for Police and Crime (MOPAC) has adequate arrangements in place for the implementation of key changes in data protection legislation i.e. the General Data Protection Regulation (GDPR).

Key Risks to Achieving Business Objective

- A lack of appropriate planning and preparation to implement changes to data protection including compliance gap and readiness assessments
- Data governance is not transparent and is not embedded across organisation or partners leading to non- reported breaches
- Roles, responsibilities and resources for data protection are not adequately assigned to individuals
- Inadequate framework in place to understand what data is collected, why data is required and what data is used for
- A failure to identify gaps in required data held by MOPAC or third party agents to support employee, customer and partner relationships
- Inability to identify where all relevant data is held or processed
- Ill defined policy and procedures including consents arrangements
- A lack of technological tools to enforce compliance or identify and report notifiable breaches within specified period
- Data is not adequately protected or disposed of leading to loss, misuse or inappropriate disclosure
- MOPAC staff may be reluctant to provide personal details if they lack trust in data privacy and conditions to consent and choice of opt out rights

Failure to manage these risks could result in non-compliance with legislation and result in reputational damage and considerable financial penalties to MOPAC. Significant breaches could lead to a lack of trust and a failure by partners or stakeholders to share data or organisations willing to work with MOPAC

Review Objectives

We assessed the effectiveness of the control framework in place within MOPAC to support the changes to Data Protection Legislation. In particular we looked to provide assurance that:

- There is a clearly defined plan in place for implementing the GDPR framework across MOPAC in compliance with legislative and regulatory requirements.
- Adequate governance arrangements are in place including the communication of staff responsibilities and accountabilities covering the review and data management process.
- Policies and procedures are in place / being developed to support the new arrangements relating to the purpose of the collection, use, retention and disclosure of data.
- A framework is designed to ensure Privacy by Design, which identifies choice and consent and data protection impact assessment conducted to ensure compliance with GDPR.

- The location, quality and security and transmission of data are maintained adequately.
- An effective monitoring and enforcement process exists to escalate and report any non-compliance within specified timescales.

Scope

We reviewed the effectiveness of the control environment supporting the framework for the implementation of GDPR within MOPAC, including preparedness, training and staff awareness. We assessed the process in place for obtaining assurance from internal partners, third-parties and external stakeholders that personal data is processed lawfully, fairly and in a transparent manner and appropriately safeguarded and held in line with GDPR requirements.

We also reviewed the controls in place for monitoring and review of data risks that have been identified, recorded and monitored through the risk management process.

Audit Definitions

Audit Assurance

Overall Rating	Criteria	Impact
Substantial	There is a sound framework of control operating effectively to mitigate key risks, which is contributing to the achievement of business objectives.	There is particularly effective management of key risks contributing to the achievement of business objectives.
Adequate	The control framework is adequate and controls to mitigate key risks are generally operating effectively, although a number of controls need to improve to ensure business objectives are met.	Key risks are being managed effectively, however, a number of controls need to be improved to ensure business objectives are met.
Limited	The control framework is not operating effectively to mitigate key risks. A number of key controls are absent or are not being applied to meet business objectives.	Improvement is required to address key risks before business objectives can be met.
No Assurance	A control framework is not in place to mitigate key risks. The business area is open to abuse, significant error or loss and/or misappropriation.	Significant improvement is required to address key risks before business objectives can be achieved.

Actions

High priority	0	Risk issues which arise from major weaknesses in controls that expose the business to high risk of loss or exposure in terms of fraud, impropriety, poor value for money or failure to achieve objectives. Remedial action should be taken immediately.
Medium priority	6	Risk issues which, although not fundamental, relate to shortcomings in control which expose the individual systems to a risk of exposure or loss.

DARA Team

Head of Audit and Assurance: David Esling
Group Audit Lead: Mark Woodley
Risk and Assurance Auditor: Kemi Keshiro

Individuals Consulted During the Review

James Bottomley, Head of Governance and Risk, MOPAC
Sara Cain, GDPR Project Manager, MOPAC
Sarah Egan, Corporate Administration Manager, MOPAC
Gemma Deadman, Strategy and Corporate Planning Manager, MOPAC
Amelia Zahra, HR Officer, MOPAC
Samantha Macleod, EA to Victims Commissioner and Director IOM, MOPAC
Maxine Gordon, Contract & Performance Officer, MOPAC

Report Distribution List

Rebecca Lawrence, Chief Executive, MOPAC
Siobhan Peters, Chief Finance Officer, MOPAC
Paul Wylie, Director of Strategy, MOPAC
James Bottomley, Head of Governance and Risk, MOPAC
Sara Cain, GDPR Project Manager, MOPAC
Elliot Ball, Head of Strategic Finance and Resource Management, MOPAC
Paul Grady, External Audit