MOPAC | MAYOR OF LONDON OFFICE FOR POLICING AND CRIME | METROPOLITAN POLICE | TOTAL POLICING

MOPAC and MPS Oversight Board
5 February 2018

Information Governance in the MPS

Report by: Phil Woolf, Director of Information & Insight

---

1) Purpose of Paper

The purpose of this paper is to provide an update on information governance within the MPS and on progress to prepare for the changes to Data Protection legislation that arise from the EU General Data Protection Regulation (GDPR) and Law Enforcement Directive (LED), both being introduced in May 2018.

2) Recommendations – that the Oversight Board:

a) Review and acknowledge the challenges faced and progress made in the area of information governance and the preparations to implement the new legislation by the MPS.

3) Summary

- The MPS has robust governance in place for information management.
- The implementation of new legislation, GDPR, is challenging but we have a plan in place to address this, and DARA has conducted an audit of our approach (attached as Annex 1).
- The MPS has a constructive working relationship with the regulators in the area of information governance. This includes inviting the Information Commissioner's Office (ICO) to conduct a series of audits of MPS governance structures.
- We have addressed the issues raised by previous London Assembly Oversight Committees.

4) Information Governance

a) Information governance is led at Management Board-level within the MPS and is highlighted as a risk on the corporate register:
"Poor information management leading to a lack of knowledge of what information we have and where it is stored, resulting in our information not being trusted, accessible, useable or legally compliant".

b) The Senior Information Risk Owner (SIRO) within the MPS is the Assistant Commissioner Professionalism. AC Ball chairs the Information Assurance & Security Board (IASB), which tests assurance around the governance and security of Met information and assets and directs activity. IASB reports quarterly to Risk & Assurance Board.

c) Existing governance is being strengthened by identifying Information Asset Owners at senior level to ensure we have oversight and ownership of all MPS systems and information. Preparations are in hand to ensure that these role specific asset owners are briefed and trained in their responsibilities.

d) At present we are working with colleagues across the Met to finalise an Information Asset Register. For every type of information (crime records for example) we need to document the legal basis for processing; when and how we share that information; any disclosure of information overseas; whether we rely on the consent of the individual to process their personal data; and our approach to records management. This Register will help us understand how much additional work is required for compliance. It will also enable us to identify systems that won't be replaced by our new MiPS system (which will cover intelligence, investigation, custody and case management).

e) IASB is briefed on the MPS' progress on Review, Retention and Disposal (RRD): ensuring we have and implement a policy for which information we keep. The Board has agreed a policy in line with national Authorised Professional Practice. Operation Filesafe is reviewing millions of paper records stored in MPS buildings, supporting the work to reduce and make better use of the estate. In the future MiPS will make a substantial and positive difference to RRD for new information. Dealing with existing data across multiple, legacy IT systems is challenging and will be reliant on the Information Futures Programme within the Portfolio.

5) GDPR

a) The UK Data Protection Bill 2017 is progressing through the various legislative stages and will be implemented in May 2018. This will bring the UK in line with two new pieces of EU law, the General Data Protection Regulation (GDPR) and Law Enforcement Directive (LED). The police service is already well

placed to meet the requirements but additional work and some resource are needed to make us compliant. There are several challenges around the new legislation with regards to information governance. These include the need to implement two regimes: one covering personal data such as HR records and occupational health data about our officers and staff; the other personal information used for a policing purpose, such as a victim's details on a crime record. We are working closely with national colleagues on policing's preparations for the new legislation and are represented on the NPCC National GDPR Reform Group headed by Commissioner Ian Dyson, City of London Police.

b) Delivering on the MiPS Programme and agreeing the scope and funding of the Information Futures Programme will provide us with the capability to improve our data quality and enable us to deliver our RRD policy.

c) The legislation, coupled with the ICO's intentions to raise public awareness of individuals' information rights, may lead to an increase in people requesting copies of their personal data. The time allowed to process these requests will also reduce from 40 calendar days to one calendar month. We received 3,700 of these "subject access requests" in the last year and current Met resources – which of course have to be balanced across a spectrum of functions to keep London safe – struggle to meet existing demand and deadlines, even though working practices have been reviewed and refined.

d) A business case is currently being prepared to replace the case management IT system MetRIC used within the MPS to manage the high volumes of data protection subject access requests (SARs) and Freedom of Information Act (FoIA) requests.

e) In 2017 the MPS received a total of 3,865 FoIA requests. Across Government departments and agencies only a very small number experience higher demand. At the time of writing (mid-January 2018) 91% of the MPS' 2017 requests had been completed. The majority of those outstanding were received in November and December. Of the completed requests, 51% were answered within the statutory 20 working days and 86% within 40 working days. Only 61 cases (1.7%) exceeded 80 days. The Act allows some cases to exceed 20 days, for example if the MPS is seeking clarification from the person who submitted the request, so compliance will be slightly higher than 51%. We are working to improve our speed of responding to requests, and know that compliance impacts on our transparency agenda and our ability to gain the trust of the public. We have an action plan in place and the ICO is briefed monthly on our compliance. IASB is made aware of both SAR and FoIA compliance as a standing item.

6) Audits

a) The MPS processes some of the most sensitive personal information but also has both a legal requirement and a commitment to be as lawfully transparent as possible. In order to achieve this balance, since 2011 we have invited the Information Commissioner's Office (ICO) to conduct five consensual audits and reviews of information management in the MPS.

b) The 2011 audit was one of the first of its kind for policing and covered data protection governance, training and awareness, and subject access requests for personal data. This report found the MPS had clear lines of reporting and escalation; relevant policies and procedures in place; and a mandatory data protection training package.

c) In 2016 and 2017, three further data protection audits returned to SARs, training and governance and also examined security of personal data. The majority of actions from all of these audits have now been closed. There were some recommendations, such as the ICO's proposal of annual training for all staff, that we have chosen not to implement. In the training example we are rewriting our mandatory package for all staff, and supplementing it with role and system specific training and briefing as required.

d) In May last year the MPS Commissioner met the Information Commissioner who offered the ICO's assistance in reviewing our FOI processes given the pressures on performance. The ICO team reported they were impressed by the motivation of MPS staff and the working practices and processes they found. Their only recommendation for improvement was replacing the MetRIC IT system.

e) Last year DARA conducted an audit on the Met's preparation for GDPR and LED. The outcome was Adequate assurance, the auditor noting:

> *"An adequate planning framework has been developed in preparation for the changes to Data Protection Legislation, and in particular to achieve compliance over consent, fair processing and contractual compliance. However, compliance over review, retention and deletion will not be fully achieved until Met Integrated Policing Solution (MiPs) and Information Futures (IF) are implemented under longer term solutions as part of One Met Model transformation."*

7) Met engagement with the Regulators

a) <u>Information Commissioner:</u>
The MPS has a constructive working relationship with the ICO that involves regular meetings and contact with the Group Manager, Police Justice & Borders and members of her team. This relationship means that we are able to discuss issues and trends in a very open and productive manner. This

relationship also gives the ICO confidence that the MPS is a willing partner in the area of information compliance.

b) Investigatory Powers Commissioner's Office**,** formally the Surveillance Commissioners:
SCO39 Covert Governance and Intelligence Compliance act as the contact point for this body, communicating on a daily basis to manage authorities and also on an annual basis to manage their inspections with the organisation. SCO39 also manage the investigation of any breaches of the legislation, conducting a review of the activity and implementing any required process changes. SCO also carry out internal reviews and inspections throughout the year.

8) GLA Oversight Committee and Facial Recognition

a) The GLA Oversight Committee met on 14 September to scrutinise the GLA Group's use of personal data. It was critical of the MPS' trial of facial recognition.

b) Although not yet a legal requirement, the MPS has actively engaged with the ICO on the production of Privacy Impact Assessments (PIA) on several major projects including facial recognition as well as Body Worn Video (BWV), drones and ANPR data. These initiatives could be considered contentious by both the regulator and the public however, by ensuring that the PIAs are living documents that address the risks raised, the public and oversight bodies can be assured that the personal data 'captured' is processed in accordance with legislation. These areas are fast moving and the MPS is making full use of new technology whilst, through PIAs, clearly safeguarding the rights of the individual.

c) The MPS' trial of facial recognition involves testing the technology on live images at ten operational deployments in a range of different environments and scenarios. Images from cameras, specifically deployed for the trial, are streamed directly to the facial recognition system, which contains a 'watch list' of individuals. The list is bespoke to every deployment, taking into consideration factors such as the specific operation, associated crime analysis, geography and intelligence. A match above threshold between a live image and the watch list generates an alert and presents both pictures to an officer. They can then make a decision about the most appropriate action, such as intercepting and stopping the individual, confirming their identity (using other means) and if necessary making an arrest. Detected faces that do not generate a match are discarded from the facial recognition system in real time. Matched images and recorded footage are deleted after three months.

d) Before the first deployment the MPS engaged with the offices of the Information Commissioner, Surveillance Camera Commissioner and the Biometrics Commissioner, and with Big Brother Watch, briefing them on the purpose and parameters of the intended trial. Both Liberty and Big Brother Watch attended Notting Hill Carnival 2017, were given an extensive briefing and witnessed the technology being used in a live operation. Whilst a full public consultation has yet to take place, more than 10,000 leaflets have been handed out to people attending Carnival over the past two years. They include an email address for the public to contact us and allow their views to be known. To date we have received no emails. At the Cenotaph in November police were present and visible with the same leaflets. The public's comments were overwhelmingly positive with regards to use of facial recognition. Also, in December 2017 the MPS met with the Biometrics and Forensics Ethics Group established to provide independent advice to the Home Office.

e) It has always been the intention to publish the trial results and hold a public consultation once all the data is available to allow an informed debate to take place. This was written into the original PIA, which was extensively discussed with the ICO and provided to all the commissioners.

f) BWV is now used, with correct oversight and legal considerations, to the benefit of not only the MPS but also the wider community, with London's Community Monitoring Network viewing recordings of stop and search.

g) There is also a balance to be drawn between the rights of the individual and the rights of the wider public. The proof of concept trial of facial recognition at Notting Hill Carnival highlights this dilemma. The checks and balances on site meant that we were confident that the technology, combined with the correct level of human intervention, was being used to protect the thousands of people visiting Carnival.

h) With ANPR, the MPS has been actively engaged with the national group, providing data protection advice and expertise. Retention periods for ANPR are now set at 12 months unless there is a justified requirement to retain data for longer.

9) Conclusion

Good information management is one of the essential building blocks of policing. It is a moral, fiscal and operational imperative that the MPS achieve its ambition of becoming a data driven organisation. This can only be realised by good information management at all levels of the MPS and our interactions with trusted partners. It is also vitally important that we take the people we serve and the police family on that journey with us: this can only be accomplished by them having confidence in the way that we handle the most sensitive of personal data under all conditions.

Directorate of Audit, Risk and Assurance
Internal Auditors to the MPS

Risk and Assurance Review
December 2017

Preparation for Data Protection Changes- General Data Protection Regulations (GDPR)/Law Enforcement Directive

METROPOLITAN POLICE

TOTAL POLICING

Executive Summary

1. Background

1.1 The purpose of our review is to provide assurance on the preparedness by the Metropolitan Police Service (MPS) to demonstrate compliance with data protection legislation and Management of Police Information (MoPI -2005) as a result of the and changes to data protection legislation, primarily the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED).

1.2 The principles of GDPR apply to the existing Data Protection Act (DPA) for 'personal data' but GDPR defines more clearly personal identifiers and includes manual and automated personal data held and processed. For the purposes of law enforcement the LED applies to the MPS.

1.3 The GDPR/LED will come into effect in May 2018 and the United Kingdom (UK) Data Protection Bill to align with European Legislation, regardless of the UK's decision to leave the European Union is at Committee stage in the House of Lords. Non-compliance with GDPR/LED could lead to significant fines and reputational damage to both data 'controllers' and 'processors'.

1.4 The GDPR has defined data controllers and processors to identify roles, responsibilities and legal obligations. This impacts on organisations such as the MPS who maintain large amounts of personal data and have also outsourced functions such as IT, Occupational Health, Finance, Human Resources and Procurement.

1.5 In 2015, Her Majesty's Inspectorate of Constabulary (HMIC) inspected and reported on the MPS and other police forces with 'Building the Picture' – An inspection of police information management. Whilst one recommendation was completed, four of the five recommendations made by HMIC are still being progressed primarily due to a lack of integrated IT infrastructure affecting the Review, Retention and Deletion (RRD) of information leading to areas of non-compliance with MoPI.

1.6 We completed a review of Operation Filesafe in July 2017 which looked at the management of paper files and are also conducting a follow up review of the Data Security Assurance Framework for third party data processors for outsourced contracts completed in March 2017 and this will be reported separately.

2. Audit Assurance

Adequate

An adequate planning framework has been developed in preparation for the changes to Data Protection Legislation, and in particular to achieve compliance over consent, fair processing and contractual compliance. However, compliance over review, retention and deletion for GDPR and MoPI will not be achieved until Met Integrated Policing Solution (MiPs) and Information Futures are fully implemented under longer term solutions as part of One Met Model transformation.

3. Areas of Effective Control

Executive Summary

3.1 The Head of Information Law and Security chairs monthly GDPR workshops involving subject matter experts from the Information Assurance Unit (IAU) and the Directorate of Legal Services to contribute to and review progress of the Data Protection Reform Police Service Implementation Plan. The plan includes the compliance requirement, vulnerability, action owner and Red, Amber Green (RAG) status for each requirement to meet compliance.

3.2 Information management/security risk is on the corporate risk register and is being redefined to separate the security element. However, the current risk description clearly defines MPS vulnerabilities in relation to what information known about and how it is stored, used and accessed and issues of legal non-compliance.

3.3 GDPR preparedness is a standing item at the monthly IASB chaired by the Assistant Commissioner Professionalism in her role as the Senior Information Responsible Officer (SIRO). Portfolio and Investment Board (PIB) and Management Board (MB) have been updated by the SIRO on MPS preparedness for GDPR.

3.4 In the medium term MiPs is intended to deliver a single integrated, unified, operational policing system that managed information end to end business policing processes in relation to custody, intelligence and case management. The refreshed MiPS Outline Business Case was approved by the Mayor Office Policing and Crime (MOPAC) Investment Advisory Board (IAB) in October 2017 and the project continues to progress towards Full Business Case and contract award. Once implemented from 2019/2020 MiPS will deliver capability for RRD and assist in demonstrating compliance with GDPR/LED and MoPI for 7critical systems.

3.5 In October 2017, PIB made a decision to take Information Futures to a Strategic Outline Case (SOC) for April 2018. In the longer term Information Futures should shape the MPS into a more data driven organisation and improve the management and storage of data resulting in greater data protection compliance.

3.6 An Information Asset Register (IAR) is being developed by the Information Security Officer (ISO) to identify all relevant information systems and their Information Asset Owners (IAOs) who have specific obligations under GDPR. Compliance will be monitored through the IASB. However, there will be an ongoing requirement to maintain, update and review the IAR as an effective management tool.

3.7 The MPS is engaging with the National Police Chiefs Council (NPCC) and National Counter Terrorism Police Headquarters (NCTPHQ) over data protection reform to identify SIRO responsibilities and obligations within law enforcement as data controllers.

3.8 Staff awareness is important in ensuring compliance and in October 2017, an operational notice was issued on the MPS intranet to inform MPS staff, and officers about GDPR. This will be reinforced by further awareness information issued by the IAU. However, cultural change will also be required to embed behaviour regarding managing information at all levels in the organisation.

3.9 The MPS is assessing a data maturity model to benchmark current data management activities against the One Met Model (OMM) transformational objectives. The model

identifies where organisations may feature based on criteria from 'Aware' to 'Managed' and includes an assessment of compliance benchmarking as part of the maturity assessment.

4. Key Risk Issues for Management Action

4.1 The 2015 MPS Information Management Strategy (IMS) is due for review in 2018. However, key aspects of the IMS cannot be fully implemented and whilst work is taking place to prepare for GDPR and LED, significant challenges remain to ensure longer term compliance and mitigate existing exposure and vulnerabilities. By May 2018, the MPS will not be fully compliant for RDD in relation to GDPR/LED or MoPI.

4.2 Significant longer term transformation of Information Futures and MiPS under the OMM will enable improved use and reliability of MPS data and will also assist in demonstrating legal compliance as regards data protection around information management including MoPI. However, until MiPs and latterly Information Futures are implemented, the MPS is vulnerable to litigation, enforcement action and criticism for legal non-compliance.

4.3 The Information Commissioner's Office (ICO) is monitoring MPS performance and is aware of current non-compliance timeliness for Freedom of Information (FOI)/ Subject Access Request (SARs). GDPR will shorten compliance timescales and a review of resources in the Information Rights Unit (IRU) has identified capacity shortfalls which would require the recruitment of additional staff. Non-compliance could lead to ICO penalties/enforcement action and separate litigation from individuals or class actions for failing to respond to data requests within prescribed timescales.

4.4 The MetRIC case management system used for the management of correspondence FOI/SARs is obsolete and will require a significant reconfiguration to meet the reduced time scales under GDPR. A compliant replacement system is being considered as a solution; however formal agreement to procure and implementation will be required prior to May 2018.

4.5 The Head of Information Law and Security is retiring from the MPS shortly and it is important that leadership and continuity of the Data Protection Reform Police Service Implementation Plan is maintained to ensure delivery of the plan prior to GDPR implementation.

Key Findings and Agreed Action(s)

1. GDPR -Preparedness Plan

Finding	Risk	Agreed Action(s)
The Head of Information Law and Security chairs monthly GDPR workshops involving subject matter experts from the Information Assurance Unit (IAU) and the Directorate of Legal Services to contribute to and review progress of the Data Protection Reform Police Service Implementation Plan. DARA were also invited to the workshops by the Chair to help form an opinion of the adequacy of the arrangements in place for this review. Using a nationally agreed NPCC template, the preparedness plan is based upon the Information Commissioner's Office (ICO) 12 steps to prepare for GDPR. The template includes the compliance requirement, the vulnerability, action owner and Red, Amber Green (RAG) status. It is designed to consider all aspects required to demonstrate compliance with GDPR. These are: • Awareness • Information you hold • Communicating privacy information • Individuals' rights • Subject Access Requests • Legal basis for processing personal data • Consent • Children • Data breaches • Data protection by design and data protection impact assessments • Data Protection Officers • International The template/plan has identified action owners and national and MPS positions which are reported to and taken up by appropriate individuals/boards in the MPS or the NPCC working group. However, it is recognised at this stage, the MPS will not be compliant by May 2018 with all aspects of GDPR/LED or MoPI in particular capability around	Fines and reputational damage to the MPS for non-compliance with GDPR/LED.	1.1The Data Protection Reform Police Service Implementation Plan forms the basis of effective planning for the MPS to identify risk areas and consider appropriate management actions. The recruitment of additional staff within the Information Rights Unit is being addressed. 1.2 The MPS accepts that it will not be fully compliant with MoPI and GDPR/LED by May 2018. However, where possible Information Management risk is being mitigated and plans for future compliance are being developed as part of OMM transformation. The SIRO as chair of IASB will continue to

Key Findings and Agreed Action(s)

Finding	Risk	Agreed Action(s)
Review, Retention and Disposal of information across MPS systems. (MoPI was introduced since 2005 as a result of the Bishard Inquiry into the 2002 Soham murders where the management of police information was severely criticised.) Information management has been assessed as high risk on the MPS corporate risk register and a requirement of OMM transformation is to at least deliver the required legal compliance. Until the MPS is able to implement its ambitions around being a data driven organisation including demonstrating compliance, the MPS remains vulnerable to criticism, financial penalties and a lack of trust in its management of personal data for policing purposes. The MPS is in regular contact with the ICO who is responsible for enforcement of data protection legislation and who has conducted recent audits MPS compliance. The ICO is aware of longer term plans for technological transformation solutions as part of OMM including Met Integrated Policing Solution (MiPs) and Information Futures. However, these transformational objectives would need to be in a reasonable timeframe to offer credible mitigation against enforcement action or fines for persistent non- compliance with data protection legislation. The ICO has monitored MPS performance of current non-compliance timeliness for Information Freedom of Information/Subject Access Request (SARs). In 2016, the MPS dealt with 3,700 information requests but did not always comply with timeliness requirements due to a lack of capacity. The resources and working practices of the Information Rights Unit (IRU) have been reviewed to match the proposed reduction from 40 days to one month to deal with Subject Access Requests (SARs). Recruitment of additional staff would be required against a backdrop of reducing budgets and decisions are required to consider non-compliance risk against increased staffing costs in the IRU. However, vulnerabilities because of capacity and increased public awareness of GDPR/ FOIA may also lead to deliberate targeting of the MPS for financial gain or reputational damage either on an individual or class action basis.		monitor the implementation of the plan and inform Management Board of progress and risk issues.

Key Findings and Agreed Action(s)

Finding	Risk	Agreed Action(s)
The MetRIC case management system used for the management of correspondence FOI/SARs is obsolete and will require a significant reconfiguration to meet the reduced time scales under GDPR. A GDPR compliant replacement system being considered as a solution, however a procurement and implementation process will be required prior to May 2018.	Inability to manage data requests leading to non-compliance with FOIA/GDPR legislation.	1.3 The IAU is working with DP to identify alternative solutions to replace MetRIC to improve reliability and business processes.
		Responsibility: 1.1 and 1.3 A/Head of Information Law and Security **1.2 AC Professionalism (SIRO)**
		Deadline: Monthly ongoing review at IASB

Key Findings and Agreed Action(s)

2. Governance Arrangements - High Priority

Finding	Risk	Agreed Action(s)
The Head of Information, Law and Security is the MPS Data Protection Officer and his post is appropriately structured within Strategy and Insight (MetHQ) and currently chairs the GDPR working group. The incumbent is due to retire from the MPS shortly and it is important that a suitable replacement is recruited to ensure continuity for the delivery of the GDPR preparedness plan. The Information Assurance Unit (IAU) includes the Information Security Officer (ISO), the Head of Records Management and the Head of Information Rights and appropriately all report to the Head of Information, Law and Security. They play key roles in the risk management framework for information Management and are members of the GDPR working group. The role of the Senior Information Responsible Officer (SIRO) in relation to data protection compliance is assigned to the Assistant Commissioner Professionalism who chairs the monthly Information Assurance Security Board (IASB) and discusses information management risks and GDPR preparation as standing agenda items. The SIRO has briefed Management Board in a paper dated 15 September 2017 and identified the key changes in legislation, potential resource implications for compliance, co-operation and liaison with the NPCC, Government departments and ICO and highlighting that GDPR hold personal responsibility for all staff and officers. The MPS is engaging with the National Police Chiefs Council (NPCC) as part of the data protection reform working group. This involves other police forces, the Home office, Department of Digital, Culture Media and Sport (DCMS) and the Information Commissioner's Office. The National Counter Terrorism Police Headquarters (NCTPHQ) and the MPS are in discussion over data protection reform to identify responsibilities and obligations within law enforcement. This will clarify legal responsibilities as SIROs and data controllers under a Section 22 Agreement. This formal engagement is documented within the preparedness plan and key issues escalated through the IASB.	Fines and reputational damage to the MPS and non-compliance with FOIAGDPR/LED and MoPI if a replacement DPO is not recruited in a timely manner.	2.1A recruitment process is in place to recruit a suitably qualified replacement for the Head of Information, Law and Security. The Head of Information Rights will act as Interim/ Head of Information, Law and Security to ensure business continuity until the replacement officer is in place.

Key Findings and Agreed Action(s)

Finding	Risk	Agreed Action(s)
		Responsibility:2.1 Director, Strategy and Governance
		Deadline: January 2018

3. Policies and Procedures – High Priority

Finding High	Risk	Agreed Action(s)
The 2015, MPS Information Management Strategy (IMS) is due for review in 2018 after discussion at the October IASB. However, key aspects of the IMS cannot be fully implemented and whilst work is taking place to prepare for GDPR and LED, significant challenges remain to ensure longer term compliance and mitigate existing exposure and vulnerabilities for RDD in relation to GDPR/LED or MoPI. The approved Records Management Policy Toolkit in place since January 2015 is due for review in March 2018. As with the IMS, aspects of the toolkit in relation to RRD remain non compliant with data protection legislation until a technological solution is introduced. The Information Asset Register (IAR) is nearing completion and being verified by the Information Security Officer (ISO) to identify all relevant information systems and their Information Asset Owners (IAOs) who have specific obligations under GDPR. This is a key initiative to improve information management as part of the Information Management Strategy (IMS). It will help identify the legal basis for processing and sharing data, including overseas disclosure and whether consent is required from individuals. However, there will be an ongoing requirement to maintain, update and review the IAR as an effective governance tool and this responsibility will need to be defined and implemented. The IAR will also form the basis of the MPS Systems of Record which will be used to identify all IS/IT systems and improve governance over shadow and silo systems that may not be GDPR compliant or formally assessed in terms of vulnerability or business criticality.	Fines and reputational damage if IAOs fail to comply with their obligations under GDPR/LED and the IAR is not kept fully up to date.	3.1Upon final verification of the IAR, a process to maintain the IAR will be developed by the Information Security Officer.

Key Findings and Agreed Action(s)

Finding High	Risk	Agreed Action(s)
The IRU is undertaking Data Privacy Impact Assessments as part of the preparations of GDPR to identify and mitigate risk across MPS business groups. Whilst not complete, work continues to identify triggers for business users to respond to for individual privacy and compliance as new systems are developed. Consent issues around the wording of cautions require changing following GDPR/LED and will also require communications and training to reinforce the message. This is being taken forward in the preparation plan. Fair Processing Notice is a key change in data protection legislation and means that a MPS notice should be understandable by a thirteen year old. The Head of the IRU has consulted on a draft Privacy Notice and is proposing trailing trailing the document at a school for feedback and comment. We have reviewed the document and consider it suitable and appropriate. Staff awareness is vital to GDPR compliance and an operational notice has been issued and is available on the corporate intranet to raise awareness of changes to data protection legislation. However, a further awareness literature is planned by the IAU to inform all relevant stake holders of their obligations under the new legislation once implemented.		
		Responsibility:3.1 Information Security Officer
		Deadline: January 2018

Key Findings and Agreed Action(s)

4. Third Party Assurance- High Priority

Finding	Risk	Agreed Action(s)
Victim Support Referrals have been identified as an area requiring review within the MPS GDPR preparedness plan and are now a MOPAC responsibility for the Victims Commissioner. A MPS policy is in place for victim care; however there is a need to ensure MOPAC processes are aligned to ensure compliance and identify any potential gaps in governance over data protection. A reform to the police complaints and disciplinary systems as part of the Policing and Crime Act 2017 will impact on MOPAC in the restricted use of access and licences to a National System being adopted by the MPS. The legislation gives MOPAC a formal responsibility over police complaints and there will be a requirement to formalise data protection processes to ensure information is maintained securely and used appropriately with responsibilities and accountabilities are clearly defined. MOPAC are represented at delivery group meetings and have identified user requirements but it is important to capture risks and mitigating actions under the wider MOPAC GDPR preparedness planning process. DARA have advised the MOPAC Director of Strategy who is leading on the MOPAC GDPR preparedness plan and a Project Manager has now been appointed to deliver the MOPAC GDPR plan. The GDPR has defined data controllers and processors to identify roles, responsibilities and legal obligations. This impacts on organisations such as the MPS who maintain large amounts of personal data and have also outsourced functions including IS/IT delivery, Fleet, Occupation Health, Finance, Human Resources and Procurement. Outsourcing arrangements for key outsourced and new contracts are being reviewed under the preparedness plan to ensure that GDPR requirements are in place or being progressed to ensure the obligations of data processors are	Fines and reputational damage to the MPS/MOPAC for non-compliance with GDPR/LED.	4.1 MOPAC will review their responsibilities with the MPS for GDPR/LED for Victim support referrals as part of their preparedness planning for GDPR. 4.2 MOPAC will ensure that the GDPR aspects for the police complaints and disciplinary systems are fully addressed in their preparedness planning and will liaise with the MPS as required.

Key Findings and Agreed Action(s)

Finding	Risk	Agreed Action(s)
being met. This matter is being reported on separately in our follow up report on Data Security Assurance. Existing procedures exist to report data breaches to the ICO; however, GDPR requires serious breaches to be reported within 72 hours. This includes data controllers and data processors and the MPS is working on this aspect as part of its preparedness plan.		
		Responsibility: 4.1& 4.2 Director of Strategy (MOPAC)
		Deadline: February 2018

REVIEW OF PREPARATION FOR DATA PROTECTION CHANGES TO LEGISLATION (GENERAL DATA PROTECTION REGULATION -GDPR)

DRAFT TERMS OF REFERENCE

Business Objective

Arrangements are in place for the Metropolitan Police Service (MPS) to prepare for key changes in data protection legislation i.e. the General Data Protection Regulation (GDPR) and the Police and Criminal Justice Data Protection Directive.

Key Risks to Achieving Business Objective

- A lack of appropriate planning and preparation to manage 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 the MPS 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
- 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 the MPS
- Data is not adequately protected or disposed of leading to loss, misuse or inappropriate disclosure
- MPS officers and 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 financial penalties to the MPS.

Review Objectives

We assessed the effectiveness of the control framework to support the changes to Data protection Legislation. In particular we are looking to provide assurance that:

- There is a clearly defined preparedness plan to implement GDPR and the Police and Criminal Justice Data Protection Directive

- Adequate governance arrangements are in place including responsibility accountability, review and approval
- Policies and procedures are in place 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 and identifies choice and consent.
- The location, quality and security and transmission of data are maintained adequately
- A monitoring and enforcement process exists to escalate and report any non compliance within specified timescales

Scope

We will review the control environment supporting the framework for the implementation of GDPR and the Police and Criminal Justice Data Protection Directive. The GDPR will not apply to personal information processed for national security or law enforcement activities. However, we will assess the mechanisms to the support activities undertaken by the MPS such as Finance and Human Resources including third party agents, and to activities conducted by non-police partners. We will also follow up on the review of Data Security Assurance Framework issued in March 2017. This reviewed outsourced service providers -DHL for the National Uniform Management System (NUMS), Shared Services Connected Limited (SSCL) to deliver the Police Standard Operating Platform (PSOP) for back office services and Service Integration and Management Model (SIAM) coordinated by Atos to deliver IT services to the MPS.

Audit Approach

- Discussing and agreeing the terms of reference with management.
- Identifying key risks to achieving business objectives and evaluating the effectiveness of the controls in mitigating those risks.
- Giving an assurance on the extent to which the control framework mitigates key risks and identifying any improvements.
- Issuing interim reports if areas of significant importance arise during testing.
- Discussing findings and identified risks with line management and agreeing actions to address the risks.
- Issuing a draft report to senior management to confirm acceptance of an agreed course of action prior to the issue of the final report.
- Issuing the agreed final report to AC Professionalism and the Director Commercial and Finance, copied to the MOPAC Chief Executive Officer, the MOPAC Chief Financial Officer, and the District Auditor.
- Conduct a follow up review 6 months after the issue of the final report to give an updated assurance on the control framework.

DARA Team

Group Audit Lead: Rob Davies
Risk and Assurance Auditor: Joseph Mensah

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	4	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	0	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

Group Audit Lead, Rob Davies
Risk and Assurance Auditor, Joseph Mensah

Individuals Consulted During the Review

Helen Ball, Assistant Commissioner Professionalism and SIRO
Alison Newcomb, Deputy Assistant Commissioner, Transformation
Roisha Hughes, Director Strategy and Governance
Phil Woolf, Director Information and Insight
Aimee Reed, Senior Responsible Officer, Transformation
Bob Farley, Head of Information Security and Law
Vince Freeman, Information Security Officer
John Potts, Head of Information Rights
Ian Leslie, Head of Records Management
Kurt Petchi, Solicitor Directorate of Legal Services

Report Distribution List

Helen Ball, Assistant Commissioner Professionalism and SIRO
Angus McCallum, Chief Information Officer
Alison Newcomb, Deputy Assistant Commissioner, Transformation
Aimee Reed, Senior Responsible Officer, Transformation
Roisha Hughes, Director Strategy and Governance
Phil Woolf, Director Information and Insight
John Potts A/Head of Information Security and Law
Lynda McMullan, Director of Commercial and Finance, MPS
Rebecca Lawrence, Chief Executive, MOPAC
Paul Wylie, Director of Strategy, MOPAC
Siobhan Peters, Chief Finance Officer, MOPAC
Paul Grady, External Audit
MetHQ Strategy & Governance – Information and Insight