Audit, Risk & Assurance Committee

Date	8 September 2020
Report title	Data Protection and Data Processing
Accountable Chief Executive	Deborah Cadman, OBE Chief Executive Email: Deborah.Cadman@wmca.org.uk Tel: (0121) 214 7200
Accountable Employee	Gurmit Sangha, Data Protection Officer Email: Gurmit.Sangha@wmca.org.uk Tel: (0121) 214 7301
Report has been considered by	n/a

Recommendation(s) for action or decision:

The Audit, Risk & Assurance Committee is recommended to:

(1) To note the reporting of data protection assurance, and compliance with data protection legislation.

1. Purpose

This report provides the Committee with the Data Protection Officer's (DPO) annual assessment of compliance with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA 2018).

2. Background and data protection assurance work undertaken

During the 12 months since the last data protection report considered by the Committee there has been a continued embedding of data protection principles required by GDPR. It has seen WMCA mature in its understanding of data protection requirements, particularly in the area of identifying privacy risks, and putting in place mitigating factors.

Some key developments in improving compliance have included.

2.1 Process mapping through Information Asset Registers (IAR):
There is a regulatory requirement for organisations to understand the information assets it holds, and the way that information is processed. We now have in place sufficiently detailed IAR's for each directorate, which will be subject to continued review and development.

2.2 Development of corporate training:
GDPR not only renewed a focus on organisational responsibility but also personal responsibility. Annual data protection training was once again rolled out to all staff, the completion of which was made mandatory by the Senior Leadership Team.

2.3 Establishing a Security Steering Group:
A Security Steering Group has been established, which meets quarterly. Its objectives include ensuring information security covers all business functions, ensuring information security aligns with business goals, raising information security awareness across the organisation, and implementing decisions on security management across the organisation. The Group reports to the Senior Leadership Team.

2.4 Improving breach reporting mechanisms:
The reporting of any data protection issues has been improved, and this has seen more transparency in incidents. It will enable incidents to be more effectively addressed, and any underlying issues identified.

2.5 Review of Physical Security:
16 Summer Lane is the principle location where WMCA information assets are held. A full audit of physical security within 16 Summer Lane was conducted resulting in several changes, and a new Access Control Policy & Procedure.

2.6 Penetration testing:
A National Cyber Security Centre approved CHECK company was instructed to undertake a simulated cyber-attack against WMCA computer systems to check for exploitable vulnerabilities. The test identified the strength of WMCA defence systems, and recommendations for greater protection. A rolling programme of penetration testing is being put in place.

WMCA retained its Government backed Cyber Essentials Accreditation.

2.7 Constant vulnerability testing of websites:
A programme of regular vulnerability testing of all WMCA websites has been implemented.

2.8 Embedding of Data Privacy Impact Assessments:
We are now increasingly seeing project managers/teams engaging the DPO and undertaking data privacy impact assessments. These assessments ensure projects comply with data protection legislation once they go live and are now recognised across WMCA as a key project governance document.

3. Impact of the Coronavirus pandemic

The major impact of the Coronavirus pandemic on data protection has been the shift to working remotely. Fortunately, WMCA's movement to Microsoft 365 shortly before the outbreak of the pandemic placed it in a strong position to safely accommodate remote working.

3.1 Remote working considerations:
Remote working from home has been, for some time, an available option in many organisations. As with all data processing environments it does come with inherent risks which have to be mitigated. Proven IT and recognised good practice provide a route to archiving data protection, but arguably the controls that can be implemented in an office environment may not always be possible.

The primary GDPR requirement when dealing with home working is to have in place "appropriate technical and organisational measures to guard against the unauthorised or unlawful processing of personal data and against the accidental loss or destruction of, or damage to, personal data".

Fortunately, WMCA have for a number of years made home working available for employees. Typically, a proportion of employees have worked from home 1-2 days of the week. This meant that WMCA had already in place policies, procedures and practises to support secure remote working. Additionally, the IT and data security defences have been designed with remote working in mind. For example, in 2019 we moved away from a small emerging Bring Your Own Device (BYOD) approach to corporate issued devices only, providing greater control of the security standards on mobile devices.

However, the major impact of Covid-19 was to make home working a necessity for all, rather than an option taken up occasionally by a proportion of staff. Additionally, for many the home working environment will have changed with all members of the household likely to be at home during working hours. Three key measures have been put in place to ensure continued secure remote processing of data:

- We have renewed the training and awareness programme to ensure staff remain connected to data protection issues whilst working away from the office.
  This has included the annual mandatory GDPR training consisting of modules on working remotely with mobile devices. We have also provided direct messaging to staff on good practice when working from home, and specific requirements of our information security polices which are directly relevant to home working.
  An important factor has been explaining how the controls we have in place can be maintained in the challenging environment everyone has found themselves in.
  Annex A provides an example of the type of messaging provided at regular intervals.
- Continued and increased monitoring of WMCA cyber security defence systems has been stepped up. We are constantly monitoring and running reports on any activity across our IT estate which appears suspicious.
- Despite the measures we had in place to support home working there was initially some work required to assess the best possible platform for connectivity of staff, both between individuals and those attending meetings. This was delivered against the backdrop of some platforms being scrutinised by the media, and several organisations suffering data breach incidents. Instructions on preferred platforms, and the use of

these platforms was provided to WMCA staff. Identified high risk platforms have been blocked from operating on WMCA systems.

Notwithstanding the above it has to be accepted that some will have greater facilities to support remote working than others. A factor that will have to be considered if we see continued lengthy home working is how we audit information security across hundreds of individual environments.

We must also keep in mind that we are now moving to an increased mixed split between those working from home, and those working at 16 Summer Lane.

3.2 Physical Protection of WMCA hardware:

All WMCA issued mobile devices are encrypted. In the event of loss or theft of a device we have clear reporting requirements which will result in the device being disabled by WMCA IT technicians. This is to ensure loss or theft of IT does not result in information being compromised.

The IT team are required to keep an inventory of all issued IT kit. Records are also kept of the IT technician "signing off" that issued mobile devices have been encrypted, and the relevant security tools installed. IT can only be issued following a request made under established procedures, an adult of which is retained.

4. Areas identified for attention

There are several areas which have been recognised as requiring further attention. The following are seen as priority areas which would lead to greater assurance.

4.1 Multi Factor Authentication:

Multi-factor authentication is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism. It is the strong recommendation of WMCA's Data Protection Officer, Security & Information Risk Advisor, and Principal ICT Cyber Security Specialist that WMCA should move to multi-factor authentication. This will ensure robust access controls to WMCA systems, and thereby provide greater cyber protection.

A paper on introducing this extra protection is currently under consideration.

4.2 SharePoint and information management:

The move away from paper-based records to an almost exclusively electronically held information presents challenges. It is essential that electronic information is stored and managed in a workable library that provides long-term identification, access, recovery, and destruction. It is recognised that there is currently a gap with no overarching corporate strategy on information management. Therefore, work is beginning on bridging this gap and putting in place controls which provide working flexibility but maintain corporate control of information.

4.3 Physical storage:

The storage of paper records has been a historical issue, as it is in many public sector bodies. Whilst WMCA is not creating any significant additional paper records, it has inherited large volumes of records from Transport for West Midlands predecessor, the West Midlands Passenger Transport Executive. These records are unstructured and have not been professionally managed.

Considerable work has been undertaken to ensure that any information which is subject to data protection legislation is secured. However there remains large volumes of unstructured corporate information. Plans on how paper records are going to be held going forward have been put in place, with the sourcing of secure storage facilities. However further work is required, and addressing the management of this information continues.

4.4 Government Functional Standard GOVS 007:
In July 2020 the Government set out a suite of standards applying to security risk management, planning and response activities for cyber, physical, personnel, technical and incident management. These standards are mandated requirements which will sit alongside the Governments advice and guidance contained within the HMG Security Policy Framework.

WMCA already have workstreams, existing policies, and process to address the new functional standards. However, close partnership with directorates that have responsibility for individual mandated requirements are taking place, to ensure identified actions are completed.

4.5 Development of data protection resources:
GDPR places upon WMCA a requirement to raise awareness of data protection issues across the organisation. We currently provide annual training, ongoing awareness as issues arise, and support/advice available to all from the DPO. However, it is recognised that an internal online resource would be beneficial, as this would provide a reference point for all staff providing advice, guidance, and support on data protection issues. We are looking to have this available this year.

5. Future development and monitoring

We are now into the third year since the introduction of GDPR in May 2018, which represented the biggest legislative change in how personal data can be processed. The first stage of meeting the obligations imposed by GDPR was to implement GDPR changes into WMCA policies, procedures and operations. The second stage has been imbedding those changes and new requirements for processing personal data.

The Data Protection Act specifically sets out the tasks required from a DPO. An important aspect of these tasks is the monitoring and auditing internal compliance with data protection legislation. Having worked our way through the first two stages we must now look to place a greater focus on monitoring compliance. To date this area has been focused on developing information asset registers to gain and demonstrate an organisational understanding of how data is processed across directorates. To address the wider monitoring requirements of the Act Appendix A sets out an intended programme of audit and assurance work. This will also form the basis of future reports to the Committee.

6. Summary

In summary, I regard WMCA's approach to have been robust and comprehensive. What is important though is that where gaps remain and further work identified that there is a renewed momentum and focus to properly embed good data protection practice, and a formal monitoring programme is put in place.

7. Financial Implications

N/A

8. Legal Implications

N/A

9. Equalities Implications

N/A

10. Inclusive Growth Implications

N/A

11. Geographical Area of Report's Implications

N/A

12. Other Implications

N/A

13. Schedule of Background Papers

N/A

ANNEX A:
Example of information security messaging provided to staff 2020

West Midlands Combined Authority

Stay Safe Online

Top tips for staff

It's important to understand why you might be vulnerable to cyber-attack, and how to defend yourself. The advice summarised below is applicable to your working life and your home life. You should also familiarise yourself with our Information Security and Data Protection policies and practices.

Who is behind cyber-attacks?

Online Criminals

Are good at identifying what can be monetised, for example stealing and selling sensitive data, or holding systems and information to ransom.

Foreign Governments

Generally interested in accessing sensitive or valuable information that may give them a strategic or political advantage.

Hackers

Individuals, with varying degrees of expertise, often acting in an untargeted way – perhaps to test their own skills or cause disruption for the sake of it.

Terrorists

Interested in spreading propaganda and disruption activities, they generally have less technical capabilities.

Malicious insiders

Use their access to an organisation's data or networks to conduct malicious activity, such as stealing sensitive information to share with competitors.

Honest mistakes

Sometimes staff, with the best of intentions just make a mistake, for example by emailing something sensitive to the wrong email address.

Defend against phishing attack

Phishing emails appear genuine but are actually fake. They might try and trick you into revealing sensitive information or contain links to a malicious website or an infected attachment.

- Phishers use publicly available information about you to make their emails appear convincing. Review your privacy settings and think about what you post.
- Know the techniques that phishers use in emails. This can include urgency or authority cues that pressure you to act.
- Phishers often seek to exploit 'normal' business communications and processes. Make sure you know the WMCA's policies and processes to make it easier to spot unusual activity.
- Anybody might click on a phishing email at some point. If you do, tell someone immediately to reduce the potential harm caused.

Secure your devices

The smartphones, tablets, laptops or desktop computers that you use can be exploited both remotely and physically, but you can protect them from many common attacks.

- Don't ignore software updates - they contain patches that keep your device secure. Your organisation may manage updates, but if you're prompted to install any, make sure you do.
- Always lock your device when you're not using it. Use a PIN, password, or fingerprint/face id. This will make it harder for an attacker to exploit a device if it is left unlocked, lost or stolen.
- Avoid downloading dodgy apps. Only use official app stores (like Google Play or the Apple App Store), which provide some protection from viruses. Don't download apps from unknown vendors and sources.

Use strong passwords

Attackers will try the most common passwords (e.g. password1) or use publicly available information to try and access your accounts. If successful, they can use this same password to access your other accounts.

- Create a strong and memorable password for important accounts, such as by using three random words. Avoid using predictable passwords, such as dates, family and pet names.
- Use a separate password for your work account. If an online account gets compromised, you don't want the attacker to also know your work password.
- If you write your passwords down, store them securely away from your device. Never reveal your password to anyone; your ICT team or other provider will be able to reset it if necessary.
- Use two factor authentication (2FA) for important websites like banking and email, if you're given the option. 2FA provides a way of 'double checking' that you really are the person you are claiming to be when you're using online services.

If in doubt, call it out

Reporting incidents promptly - to your ICT team servicedesk@wmca.org.uk or line manager - can massively reduce the potential harm caused by cyber incidents.

- Cyber-attacks can be difficult to spot, so don't hesitate to ask for further guidance or support when something feels suspicious or unusual.
- Report attacks as soon as possible - don't assume that someone else will do it. Even if you've done something (such as clicked on a bad link), always report what's happened.
- Don't be afraid to challenge policies or processes that make your job difficult. Security that gets in the way of people doing their jobs, doesn't work.

ANNEX B:

Data Protection Audit and Assurance Programme

		Lawfulness	Purpose	Data Minimisation	Accuracy	Retention & Storage	Security	Accountability		
GDPR		**Principle (a) – lawfulness, fairness and transparency**	**Principle (b) – purpose limitation**	**Principle (c) – data minimisation**	**Principle (d) – accuracy**	**Principle (e) – storage limitation**	**Principle (f) – integrity and confidentiality**	**Accountability principle**		**Suggested Frequency**
Data Minimisation	Review of data minimisation, anonymisation, and pseudonymisation.			X						Annually
Website Review	Review of outside facing authority website and the data protection perceptions of the service users. Accessibility, usability, consistency.	X					X	X		Annually
Incident Management	Review of the incident management process. Reporting, investigation, follow up, corporate learning etc.			X		X	X	X		Annually
Sites beyond 16 Summer Lane	Visits to WMCA sites and buildings to carry out review on physical controls, access and management controls.			X		X	X			Annually – different sites
Information asset management	Identification of information assets and defining appropriate protection responsibilities. Review of Information Asset Registers. Information classification. - Information assets are subject to an appropriate level of defence. Handling of sensitive data and controls in place.	X	X	X	X	X	X			Rolling programme across teams
Cybersecurity Risks	Cloud abuse, malware, hacking, passwords, backup. Technical vulnerability management, network security management Change management, monitoring, system acquisition, development and maintenance. Capacity management. Logging, handling security incitements.						X			Annually
Organisation of information security	Review of implementation and maintenance of information security practices. Review of mobile devices and remote working.									Annually
SARS & data subject rights	Review of the SAR and data subject rights process and how requests are processed.	X						X		Biennially
Review of the Information Governance Board	Review of the effectiveness, Terms of Reference, membership, actions and progress of the Security Steering Group.							X		Triennial
Access controls	Controls for the management of access rights of users, systems and applications, and for the management of user responsibilities			X		X				As part of project
CCTV Review	Assessment against surveillance Camera Code of Practice (SC Code).	X				X	X	X		Biennially
Information security policies review	Consideration of DP/GDPR.	X				X	X	X		Annually

Information security incident management	Controls for reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence.						X	X		Annually
Records Management Review	Storage and management of data. Review of effectiveness and data security arrangements of the Iron Mountain.			X		X	X			Biennially & As part of project
DPIAs	Data Protection Impact Assessments (DPIAs), advice and input by the DPO. Consistency, risks, actions, review.							X		Biennially
Human resources security	Controls prior to employment, during, and after the employment	X	X	X	X	X	X	X		
Physical and environmental security	Controls defining secure areas, entry controls, protection against threats, equipment security, secure disposal, Clear Desk and Clear Screen Policy, etc.						x			Biennially
Data Sharing Agreements	Review of Data Sharing Agreements in place, gaps and processes.	X								Biennially
Supplier relationships	Controls in agreements and monitoring of WMCA Data Processors.	X	X	X	X	X	X	X		Rolling programme of review
Risk Register (DPO)	Information security risk register							x		Annually