Audit, Risk & Assurance Committee

Date	29 September 2021
Report title	Data Protection & Data Security Annual Update
Accountable Chief Executive	Laura Shoaf, Interim Chief Executive
Accountable Employee	Gurmit Sangha, Data Protection Officer Email: Gurmit.Sangha@wmca.org.uk Tel: (0121) 214 7301
Report has been considered by	

1.0 Recommendation(s) for action or decision:

Audit, Risk & Assurance Committee is recommended to note the reporting of data protection assurance and compliance with data protection legislation.

2.0 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).

3.0 Overview of data protection compliance during the last 12 months

The processing of data continued to take place largely remotely with most staff working from home due to the Covid pandemic. Data protection compliance has also been monitored remotely. Whilst there are some limitations with this, we have continued to have good engagement from business areas on data protection issues. An update on data protection and lone working was presented to the Committee on 28 June 2021.

Staff have taken part in mandatory data protection training and been provided with bespoke communications setting out guidance on data protection good practise.

There has been a continued increase in WMCA business areas processing personal data engaging with the DPO and seeking advice. This has been the case both for ongoing processing and new planned processing.

4.0 Key developments

Since the last update to the Committee WMCA introduced multi-factor authentication for all WMCA IT users, which has made access controls to WMCA systems more robust. Users are now regularly requested to enter a second form of authentication in the form of a code sent to their mobile phone before access is granted. This extra layer of security is an essential recommendation of the Information Commissioners Office.

5.0 Data breaches

The number of reported data breach incidents remains low and can be grouped into three categories.

i. The cause of the majority (62%) was human (clerical) error. These breaches were assessed as low level breaches with no adverse impact on any data subjects. However, it emphasises the continued need to deliver ongoing data protection awareness to staff. Human error resulting in a data breach is always a risk. We look to mitigate this risk by continued ongoing data protection training and awareness. All incidents have been subject to specific advice and recommendations on future ways of working for the teams involved.

ii. The deployment of new IT or upgrades can present challenges due to its increasing complexity. We have seen two incidents where settings within systems has resulted in possible unauthorised access by WMCA staff who should not have permission to access this data. It should be noted that there was no risk of anyone external to WMCA gaining access. Both incidents were detected and the access issues rectified before any major breach event.

    We recognise the above highlights the need for undertaking Data Privacy Impact Assessments (DPIA) at project design and implementation stage. These assessments compel project managers to consider and record data protection risks to data that will be processed through the IT system. This should then feed into testing and further review/assessment once the system goes live.

iii. The delivery of front-line services is undertaken by WMCA through partnerships with organisations who provide specialist functions. Under data protection legislation there are two types of relationships that these partnerships form. Firstly, the partner organisation is classed as a "Data Processor" for WMCA who is the "Data Controller".

This means that they handle data on our behalf, and we are responsible for this data. Secondly the relationship may be one where both we and the partnership organisation is a "Data Controller". This means we are responsible individually for the data we respectively hold and process.

We have had reports from two partners informing us that they have been subject to a breach. We have sort and obtained assurance in relation to both incidents and are satisfied that there was no impact on any data subjects for which WMCA is responsible. The incidents highlight the need for due diligence at procurement stage, robust contractual data protection measures/requirements, and ongoing partnership monitoring.

No reported data breach incidents during the last 12 months were identified as posing a risk to data subjects or required reporting to the Regulator under the Data Protection Act 2018.

6.0 Areas requiring improvement

The focus of the DPO over the next 12 months will be on the following areas, which have been identified as requiring improvement, to increase data protection assurance:

6.1 Establishing a data protection standard to measure WMCA against

The DPO and WMCA Security & Information Risk Advisor have for some time advised that WMCA adopt an assurance standard to measure data protection compliance. The DPO and WMCA Security & Information Risk Advisor have recommended that the Government Functional Standard GOVS 007 is adopted and put in place. GOVS 007 sets out a suite of standards applying to security risk management, planning and response activities for cyber, physical, personnel, technical and incident management. These standards sit alongside the Governments advice and guidance contained within the HMG Security Policy Framework.

The DPO will continue to press for the adoption of the above.

6.2 Improving breach reporting mechanisms

The DPO will work towards improving both data breach reporting knowledge across WMCA the mechanism for reporting breaches, and breach management. The current policies and procedures will be reviewed to improve our current handling of such incidents.

This is an important aspect of data protection compliance. The legislation requires reporting to the Regulator all incidents which are reportable within 72 hours. This does not provide for a great deal of time for assessment and action. We have identified areas where our current arrangements can be significantly improved, and this will be undertaken.

6.3 Establishing a data protection resource

Maintaining data protection awareness across the organisation is vital to both ensuring compliance with legislation and preventing data breaches. Whilst we currently deliver training and data protection communications during each year, we do not have a dedicated space on the WMCA intranet which staff can refer to it. This will be established and promoted as part of filtering good data protection compliance across WMCA.

6.4 Monitoring data processing across WMCA

The final area the DPO will look to enhance is the monitoring of data processing activities across WMCA. This does currently take place, but it will be proposed to the Management Team that it is formally embedded as part of a DPO internal data protection audit plan.

7.0 General Data Protection Regulations (GDPR) Internal Audit 2021

Between April 2021 and September 2021 WMCA was subject to an internal data protection arrangements audit as part of the internal audit plan. The audit was based on the Information

Commissioner's Office data protection assurance toolkit and the auditors experience of auditing similar organisations data protection compliance.

The audit concluded a "Satisfactory" assurance over the adequacy of controls reviewed and identified several areas of good practice. The audit provided recommendations for improvement in six areas. Recommendations were given the following ratings:

GREEN - Action is advised to enhance risk control or operational efficiency
AMBER - Action is required to avoid exposure to significant risks in achieving objectives
RED - Action is imperative to ensure that the objectives for the area under review are met

7.1 Understanding what data WMCA holds and mapping how it flows (audit finding 1).

WMCA has put in place Information Asset Registers (IAR's) for each business area. These registers record the data held by the business area, how it flows through the organisation, and WMCA compliance with data protection principles.

The internal audit randomly selected registers and provided the following green rated recommendations:

- A central summary register of IAR's will be maintained to provide oversite of the registers.
- IAR reviews undertaken by the Data Protection Officer (DPO) will be resumed and completed in 2021/2022.

WMCA have a rolling programme of reviewing registers for business areas that process large volumes of personal data annually. We remain on course to complete 2021/2022. An oversite register will be put in place to provide greater clarity on the status of IAR's, and flag registers that require attention.

7.2 Ensuring data held remains accurate and up to date (audit finding 13).

Data protection legislation stipulates that personal data is accurate and where necessary, kept up to date. If inaccurate data is identified every reasonable step must be taken to erase or rectify it without delay. All business areas are reminded of this requirement and when completing their IAR's are required to confirm procedures are in place to ensure the accurate collection of data.

The internal audit provided the following green rated recommendations to improve assurance:

- The Data Protection Order (DPO) to carry out spot checks on the accuracy of data when carrying out reviews of IARs.
- To conduct regular periodic meetings between the DPO and Information Leaders within business units to communicate best data practice topics to services areas.

WMCA has implemented the above recommendations and they will be put into practise over the next twelve months.

7.3 Managing retention and disposal (audit finding 14).

The current WMCA Retention and Disposal Policy was last reviewed in 2018. Since this review there have been several changes in both retention of documents and their disposal when no longer required. This change has been heightened by the Covid pandemic which has changed the working environment, and the increasing use of electronic data instead of paper records. Therefore, in accordance with an audit green rated recommendation we will be review and update the policy.

7.4 Embedding data protection policies within WMCA (audit finding 19).

WMCA recognises that a key aspect of ensuring good data protection compliance is ensuring the organisations data protection requirements are embedded and understood by all who process data. Various channels of communication are used to deliver data protection knowledge including formal training, best practise reminders, messages and guidance. However, we do not currently have a central resource where polices, guidance, and updates can be accessed.

The internal audit provided a green rated recommendation that consideration should be given to having a dedicated webpage on the WMCA intranet site to provide a centralised point for employees to access data policies, guidance notes and new updates. A decision has been made to set up a space within the internal WMCA intranet where staff can review data protection resources to assist in processing data in a manner compliant with data protection legislation.

7.5 Appropriate technical security (audit finding 29).

The internal audit reviewed at a high level WMCA meeting the requirement of the Data Protection Act to implement technical and organizational measures that ensure a level of data security. The audit provided two recommendations:

- A green rated recommendation to consider introducing automated protective marking on e-mails.
  We will review protective marking and specifically the use of automated protective e-mail marking.
- An Amber rating to review the submission of the re- application for Cyber Essentials.

  WMCA's Cyber Essentials accreditation has expired. Whilst it is not mandatory to have such accrdiation it requires a level of security compliance which provides assurance. Both the DPO and WMCA Security & Information Risk Advisor have recommended that we reapply for the accreditation by demonstrating WMCA has in place the required standards. The matter currently sits with Digital and Data Team.

7.6 Handling data breaches (audit finding 30).

The audit provided a green recommendation that the protocol for reporting data breaches to the ICO is streamlined. As set out in 6.2 above this is planned work to be undertaken by the DPO.

8.0 Summary

WMCA continues to work towards increasing its data protection maturity. We have seen over the last 3 years a greater understanding of data protection requirements across the organisation. The last 12 months has demonstrated a continuing increase of WMCA departments considering data protection both for ongoing processing and planned new processing. We will over the next 12 months work on areas which we have identified we can develop in order to provide greater assurance and mitigate the risks identified.

9.0 Financial Implications

N/A

10.0 Legal Implications

N/A

11.0 Equalities Implications

N/A

12.0 Inclusive Growth Implications

N/A

13.0 Geographical Area of Report's Implications

N/A

14.0 Other Implications

N/A

15.0 Schedule of Background Papers

None