Audit, Risk & Assurance Committee

Date	24 September 2019
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 & Information Sharing 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

(1) To note the information set out in this report which sets out the response of the WMCA to the necessary measures complying with the requirements of secure personal data storage and processing.

1.0 Purpose

This report sets out the categories of personal data processed by the West Midlands Combined Authority (WMCA), and provides a broad overview of the data protection assurance controls in place. It also provides an outline of the regulatory action an organisation may be subject to in the event of a breach.

2.0 Background

WMCA is registered with the Information Commissioner's Office (ICO) as a Data Controller. A Data controller is legally responsible for ensuring personal data is only processed in accordance with the principals of the Data Protection Act 2018. The sixth data protection principle states that data must be kept "*secure against unauthorised or unlawful processing and against accidental loss, destruction or damage*."

Processing of personal data includes everything that an organisation may do with it, such as, collecting, storing, sharing, viewing, using, through to eventually destroying/deleting it.

3.0 Legal Implications

The implication of breaching the Data Protection Act is regulatory action from the Information Regulator, and litigation from data subjects who feel their rights under the Act have been infringed.

The Information Commissioners Office (ICO) is the UK independent regulatory office dealing with data protection and privacy issues. They undertake enforcement action through investigative action, Decision Notices, The Information Tribunal, and The Courts. Any member of the public can bring a claim to the ICO, and organisations have a legal responsibility to report data breaches to the ICO.

Additionally a data breach is likely to open claims of breaching the Human Rights Act 1998, for example to right to "private life".

4.0 Financial Implications

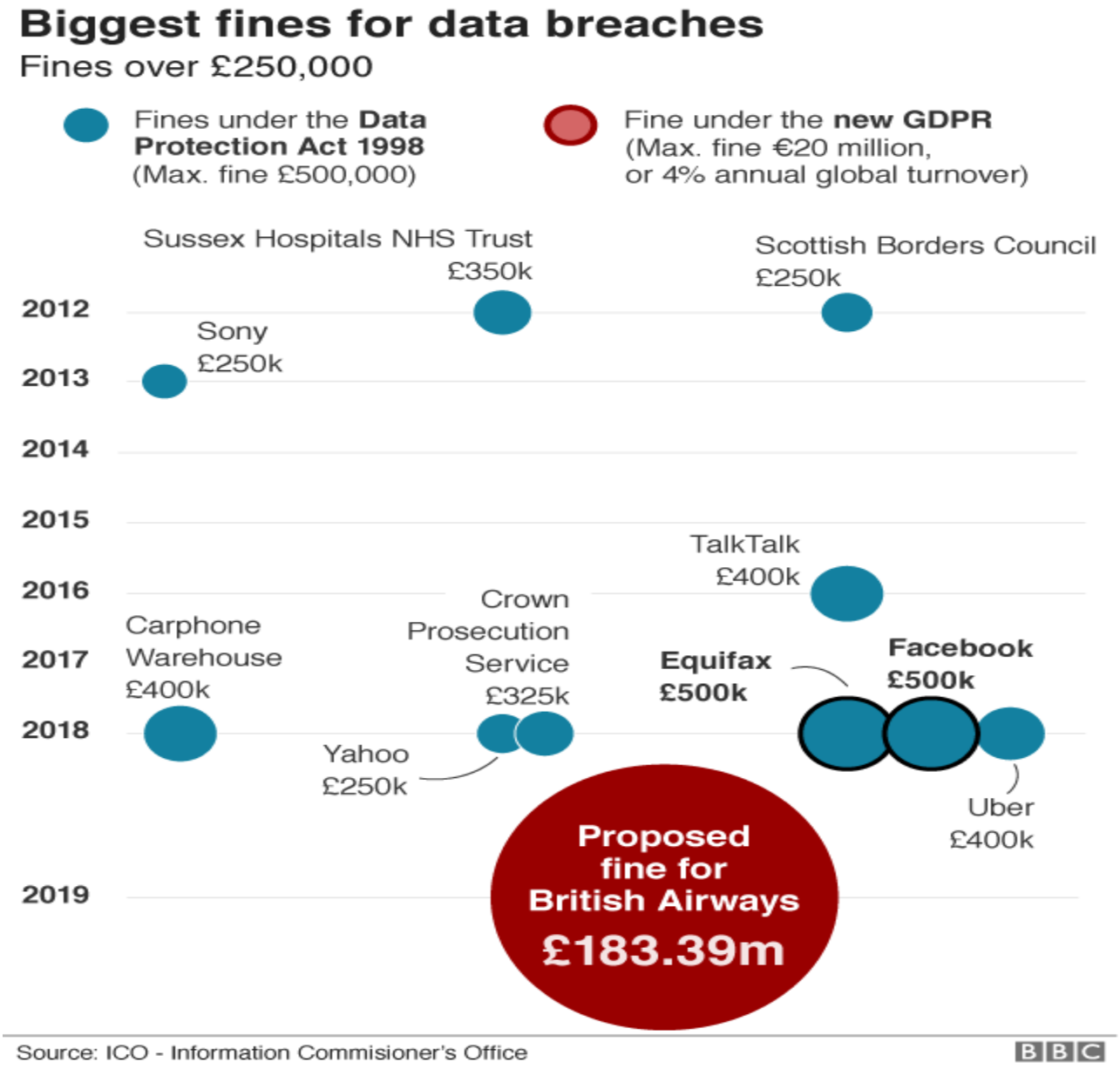
4.1 Powers of the Information Commissioners Office (ICO).

An organisation found to have contravened data protection legislation may be subject to an enforcement notice from the ICO requiring steps to be taken and/or a fine up to €20 million or 4% of an organisations global annual turnover. Additionally fines of €10 million or 2% of the turnover can be issued for failing to notify the ICO about a data breach.

Fines tend to be issued where there has been a data security breach resulting in personal data being copied, shared, transmitted, viewed, stolen or used by an individual unauthorised to do so. Examples of recent incidents resulting in fines include:

- Life at Parliament View Ltd £80,000 fine for leaving 18,610 customers' personal data exposed for almost two years.
- Hall and Hanley Ltd £120,000 fine for sending of 3,560,211 direct marketing messages to subscribers without consent.
- Bounty UK £400,000 fine for sharing personal data unlawfully with third parties including marketing agencies, and a credit reference agency.
- Uber £400,000 fine for failing to protect customers' personal information during a cyber-attack.

- Equifax Ltd £500,000 fine for failing to take appropriate steps" to protect personal data, for example keeping it to long, which resulted in a data breach following a cyber-attack.
- Facebook Ireland Ltd £500,000 fine for processing personal data of users unfairly, notably allowing App developers access to personal information without sufficiently clear and informed consent or controls.
- London Borough of Newham £145,000 fine for inappropriate sharing of information without appropriate technical and organisational controls.
- British Airways £183 million (proposed intention of ICO) fine following hackers accessing BA systems containing customer names, email addresses, payment card information, credit card numbers, expiry dates, credit card security codes.



4.2 Litigation costs

Increasing we are seeing litigation being brought by data subjects whose data has been breached. Both the Data Protection Act and the Human Rights Act permit an individual to bring a case seeking compensation if they can demonstrate the breach resulted in damage and/or distress. For example in the case of TLT v Secretary of State for the Home Department the High Court *awarded* between £2,500 and £12,500 to six asylum seekers when their personal data was inadvertently published on the Home office website.

In the majority of the above cases the data compromised amounted to customer names, contact details, a history of the services data subjects had obtained from the organisation, and transaction (banking) information.

The origins of the breaches can be summarised as a result of malicious attacks designed to cause disruption, malicious attacks seeking ransom for return of data, or employee carelessness in handling data. In each case the lack of a security control or inadequate controls resulted in improper handling of data internally, or an external operator gaining unlawful access.

5.0 Other implications

In addition to legal and financial implications a data protection breach is likely to bring negative press coverage, with the ICO publishing the fact it is undertaking any investigations, and the ultimate decision it makes on a case.

There is also likely to be a loss in confidence in any services an organisations is delivering and damage to reputation.

6.0 Personal data processed by WMCA

WMCA processes a wide range of personal data across a number of diverse areas of operation. Some key examples include.

Business area	Type of information processed	Reason for processing data
Transport for West Midlands	• names • address • DOB • National Insurance Number • telephone number • email address • Identification photographs • Information to support concessionary pass applications • Other supporting documentation and information • General enquiries • Banking – debit and credit card payments	• For the delivery of transport services and consideration of applications for: ○ Swift travel card ○ Older persons pass ○ Blind and disabled pass ○ Work wise pass ○ 16 – 18 pass ○ Student pass ○ Pass Protect ○ Direct debit services ○ Bank mandates • Customer enquiries • Customer satisfaction surveys • Credit card payments
Productivity and skills	• name • address • DOB • Education/training supporting documentation and information	• For delivery of Adult Education Budget (AEB) agenda • Monitoring of adult education providers • Delivery of Connecting Communities pilot programme • Delivery of Mayors mentors programme
Public service reform	• name • address • DOB • Work related health and wellbeing information • demographic data (age, sex, occupation etc.).	• For delivery of Thrive Into Work programme • For delivery of Thrive at Work programme • Deliver work of Mental Health Commission (This is Me)

Mayoral programmes	• Homelessness task force – names, DOB, etc. Information connected to individuals homelessness situation. • Mayors mentors – names, DOB, contact details, information on mentoring provided to young persons.	• To deliver mayoral programmes
Business area	Type of information processed	Reason for processing data
HR/Finance	• Employee information – contact details, DOB, etc • National Insurance Numbers • Banking – salary payment • Personal devolvement • Occupational health information	• To process staff employment • Handle performance
Websites	• Cookies – user tracking, and monitoring	• To deliver Website services • To deliver mobile app services
CCTV	• CCTV recordings covering bus stations, train stations, metro stops and town centres • Vehicle tracking CCTV across road network	• To deliver Safer Travel • For crime prevention
Equality data	• Special category equality data collected across all services provided	• To meet the Equality Act Public Sector Duty

Processing of data is carried out by WMCA staff, and by external partners (Data Processors). External partners are under contract with clear data protection controls, and responsibilities set out. WMCA will also share information under data sharing agreements with partner organisations.

7.0 Controls to ensure compliance with legal and regulatory requirements

WMCA has implemented and maintains a security program that leverages the ISO/IEC 27000-series of control standards as its baseline. The following specialist roles are in place to deliver data security:

1. Data Protection Officer
2. Cyber Security Specialist
3. Principal ICT Specialist - Cyber Security.

The wider ICT Team assist with providing technical security for the ICT infrastructure. The Assets Team assist with providing physical security across 16 Summer Lane.

Data security is overseen by WMCA Security Steering Group which meets quarterly, and reports to WMCA Strategic Leadership Team. The Senior Information Risk Owner (SIRO) is the Senior Leadership Team member that leads on information assurance, and has overall accountability for the management of information assets held by WMCA.

The following is an overview of the data protection controls which WMCA has put in place:

7.1 Organisational controls

- Suite of 16 information assurance, and information security management policies
- Data protection and cyber security induction for all staff joining WMCA
- Ongoing mandatory annual eLearning programme for all WMCA staff
- Reviews and audits of policies, procedures and practices
- Data Protection Officer and Cyber Security Specialist available to all staff/teams for advice and assistance

- Information security incident reporting procedure in place
- Information security risk management procedure in place
- Information Asset Registers are being established and will be subject to annual review
- Information Risk Register (IRR) in place and reviewed quarterly by Security Steering Group.

7.2 Data processing minimisation

- The amount and type of data is assessed and reviewed regularly to ensure it is no more than required

7.3 Use of specialist data processors

- Specialised partners are used when processing certain types of data, which if compromised may cause distress, harm or loss. For example when processing of credit/debit card payments, the transaction is handled separate to WMCA infrastructure by a Payment Service Provider (PSP).

7.4 Development of new processes which will involve processing personal data

Any new application, IT system, process or procedure which will involve the processing of personal data is subject to a Data Privacy Impact Assessment (DPIA) and input from the Data Protection Officer and Cyber Security Specialist. DPIA's help organisations identify and minimise risks that result from data processing.

7.5 Access Control of Processing Areas (Physical)

Web applications, communications infrastructure, and database servers are located in secure data centres. WMCA has implemented measures in order to prevent unauthorised access to the data processing equipment by:

- Establishing security areas
- Protection and restriction of access paths
- Securing the data processing equipment and personal computers
- Establishing access authorisations for employees and third parties
- Restricting physical access to the servers.

7.6 Access Control to Data Processing Systems

WMCA has implemented measures to prevent its data processing systems from being used by unauthorised persons by:

- Establishing the identification of the terminal and/or the terminal user to the WMCA systems
- Bespoke access levels for each user in accordance with their role
- Access must be approved by an appropriate manager and the "owner" for the particular system or internal application
- Automatic lock out of the user ID when several erroneous passwords are entered
- Utilizing firewall, router and VPN-based access controls to protect the private service networks and back-end-servers
- Continuous monitoring infrastructure security
- Regularly examining security risks by internal employees and third party auditors (external penetration testing)

- Passwords must adhere to the WMCA password policy, which includes minimum length requirements, enforcing complexity and set periodic resets.
- Intrusion detection systems in place.

7.7 Access Control to Use Specific Areas of Data Processing Systems

Persons entitled to use a data processing system are only able to access Personal Data within the scope and to the extent covered by their respective access permission (authorisation) and that Personal Data cannot be read, copied, modified or removed without authorisation. This is accomplished by:

- Employee policies and training in respect of each employee's access rights to the Personal Data
- Users have unique log in credentials -- role based access control systems are used to restrict access to particular functions
- Monitoring activities that add, delete or modify the Personal Data
- Release of Personal Data to only authorised persons.

7.8 Availability Control

WMCA has implemented measures to ensure that Personal Data is protected from accidental destruction or loss. They include:

- Secure backup of all systems
- Active and redundant server infrastructure is set up with disaster recovery sites. This is currently under review to ensure fitness for purpose.
- Annual testing of disaster recovery data centers
- Service level agreements from internet service providers to ensure a high level of uptime.

7.9 Transmission Control

WMCA has implemented measures to prevent Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This includes:

- Use of adequate firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
- Sensitive Personal Data encrypted during transmission using strong encryption algorithms and keys
- Certain types of customer Sensitive Personal Data and other confidential customer data (e.g. payment card numbers) are encrypted at rest within the system
- Protecting web-based access to account management interfaces by employees through encrypted Transport Layer Security (TLS).
- End-to-end encryption of screen sharing for remote access, support, or real time communication;
- Constant monitoring of threat levels and suspicious activity.

7.10 Input Control

WMCA has implemented measures to ensure that it is possible to check and establish whether and by whom Personal Data have been input into data processing systems or removed. This includes:

- Authentication of the authorized personnel
- Protective measures for Personal Data input into memory, as well as for the reading, alteration and deletion of stored Personal Data, including by documenting or logging material changes to account data or account settings
- Segregation and protection of all stored Personal Data via database schemas, logical access controls, and/or encryption
- Utilisation of user identification credentials
- Physical security of data processing facilities
- Session time out.

7.11 Monitoring and analysing risks, auditing of controls

- Data protection activity, risk levels, and threat detection is subject to monitoring internally by the Data Protection Officer, Cyber Security Specialist, and WMCA Security Steering Group, who all have responsibility to ensure secure processing of data across WMCA. Areas of security and control levels are analysed by the group on a rolling annual basis. Gaps or threats are required to be addressed and/or recommendations made to WMCA Senior Information Risk Owner (SIRO).
- The IT infrastructure is subject to external penetration testing to identify security gaps and risk levels. New IT applications will also be subject to penetration testing before they go live.
- The IT infrastructure is subject to constant reporting and analysis.
- Policies and procedures are subject to annual review

The information assurance programme will continue to operate across all areas where information is processed and will continue to evolve to meet exiting and new challenges.