Buckinghamshire & Milton Keynes Fire Authority

MEETING	Overview and Audit Committee
DATE OF MEETING	20 November 2019
OFFICER	Graham Britten, Director of Legal & Governance
LEAD MEMBER	Councillor David Hopkins
SUBJECT OF THE REPORT	**General Data Protection Regulation (GDPR) – One Year On**
EXECUTIVE SUMMARY	The purpose of this paper is to review the implementation of the GDPR across the Authority since it came into effect on 25 May 2018. The Overview and Audit Committee was last apprised of progress at its meeting in March 2019 at which it agreed that periodic progress reports on implementation progress be received.
ACTION	Noting.
RECOMMENDATIONS	That the report be noted.
RISK MANAGEMENT	Details of outstanding issues are included in the Information Management risk register. This report has no equality, diversity and inclusion implications. The report is about the implementation of privacy legislation and does not include any personal or personally identifiable information (PII). The report does cover issues of cyber security but does not introduce any new or increased threats to security.
FINANCIAL IMPLICATIONS	There are no financial issues directly associated with the report. However, risk treatments may have financial implications.
LEGAL IMPLICATIONS	There are no direct legal implications associated with this report.
CONSISTENCY WITH THE PRINCIPLES OF THE DUTY TO COLLABORATE	The report deals with implementation measures for GDPR in the Buckinghamshire & Milton Keynes Fire Authority. Opportunities to collaborate may arise as risk treatments are identified by relevant Information Asset Owners.
HEALTH AND SAFETY	There are no health and safety issues directly

	associated with this report.
EQUALITY AND DIVERSITY	Nothing in the report deals directly with issues of equality, diversity or inclusion.
USE OF RESOURCES	Any resource implications will arise directly at department / stations level. **Communication** The Information Governance & Compliance Manager, in her role as Data Protection Officer, will raise awareness of actions needed to comply with GDPR, with Information Asset Owners (Senior Management Team members) and their Information Stewards; and provides guidance and training to employees. Procedures and information security articles will be notified through the Authority's intranet.
PROVENANCE SECTION & BACKGROUND PAPERS	**Provenance** This paper has been considered by the Performance Management Board and the Strategic Management Board. **Background** Regulation 2016/679 of the European Parliament and of the Council Data Protection Act 2018 Implementation progress of the GDPR/DPA 2018 (Report to Overview and Audit Committee, 13 March 19)
APPENDICES	Appendix A - GDPR One Year On report
TIME REQUIRED	5 minutes
REPORT ORIGINATOR AND CONTACT	Gerry Barry gbarry@bucksfire.gov.uk 01296 744442

Appendix A
The General Data Protection Regulation (GDPR): One year on

The purpose of this paper is to review the implementation of the GDPR across the Authority since it came into effect on 25 May 2018.

1. *12 Steps*

Although the Authority followed the guidance from the Information Commissioner's Office (ICO) – *"Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now"* - very limited supporting guidance was available. Indeed there was (and is) no certification[1] scheme in place for organisations to demonstrate compliance to the GDPR and enhance transparency.

The Annual Governance Statement 18/19 approved by the Overview and Audit Committee at its meeting on 17 July 2019 contained an update of the Authority's progress against the '12 Steps'. The Committee approved new governance issues which were identified to be addressed in 20/19 in the area of 'Security – People, premises, information'.

2. *Monitoring compliance*

We currently monitor our compliance through a rolling programme of work which includes checking that our employees are adequately trained for their roles and that our suppliers, potential suppliers and partner agencies are also trained and able to demonstrate that they have adequate arrangements in place to protect information.

Each month the ICO advise on changes it has introduced and we review these for any impact on Authority plans or process's.

We demonstrate compliance by keeping records of what we are doing with Personally Identifiable Information (PII) and our legal basis for processing it, and by embedding privacy measures into corporate policies and everyday activities.

3. *Certification*

Following adoption of the Guidelines on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, by the European Data Protection Board (June 2019), the ICO has advised that the certification scheme will be in place this Autumn.

So, whilst a lot of work was undertaken to prepare for GDPR, post 25 May 2018 we continue to work towards compliance as it is a moving feast until sufficient case law exists to interpret some of its provisions.

4. *Data Protection Impact Assessments (DPIAs) (Article 35)*

A DPIA is required where a type of processing in particular using new technologies and is likely to result in a high risk to the rights and freedoms of natural persons (data subjects). All new or amended processes or projects undertaken within the Authority are screened to determine any privacy issues and, where the privacy issues are likely to be high risk, more detailed DPIAs are undertaken.

[1] Articles 42 and 43 talks about the introduction of a certification standard and agreed certification bodies.

5. Security of processing (Article 32)

The Data Protection Act 1998 (repealed) stated that "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, and damage to, personal data". Under GDPR not only do measures have to be taken to protect data but these measures must be designed into the systems and processes and comprehensive Records Of Processing Activity (ROPA) kept to demonstrate who information is shared with. Since GDPR came into effect all departments and Stations are required to maintain a register of all the types of information they hold, who they share it with, and other details such as how long it's held for and where.

6. Cyber

One significant change since the Data Protection Act 1998 first came into effect has been the move from predominantly paper records to electronic records and the increase in cyber-crime.

We undertake a number of measures to protect Authority systems from attack, this includes the use of intrusion detection software and patching, and we employ measures to delete records that are no longer required. This is both to reduce the risk of holding PII for longer than we can justify and to remove the opportunities for viruses to lay dormant in files.

People continue to create the prime vulnerability either through failure to take appropriate measures to protect data, being vulnerable to social engineering or being threat actors for money or beliefs.

This summer we achieved Cyber Essentials and will work toward Cyber Essentials Plus. Cyber Essentials is a Government-backed, industry-supported scheme to help organisations protect themselves against common online threats. We have internal audits of Information Security and employ Penetration Testers (aka ethical hackers) to provide assurance in the security of our IT network by attempting to breach some of the system's security, using the same tools and techniques as an adversary might[2].

7. What next for GDPR?

With the passing of the first year of GDPR, the Information Commissioner has stated that the focus for the second year of the GDPR must be beyond baseline compliance; that organisations need to shift their focus to accountability with a real evidenced understanding of the risks to individuals in the way they process data and how those risks should be mitigated. Well-supported and resourced Data Protection Officers are central to effective accountability[3]. People are increasingly demanding to be shown how their data is being used and looked after.

As cybercrime evolves, and criminals become more deceptive in their attack methods, we will need to continually address privacy and security risks to ensure we are accountable for the personal data we hold and are compliant with the legislation.

We will continue to build on our knowledge of GDPR and the impact case law has on it. We will ensure that our policies and procedures reflect good practice and that performance is monitored and reviewed at an acceptable frequency.

[2] National Cyber Security Centre definition
[3] Blog: GDPR - one year on, 30 May 2019, a blog by Elizabeth Denham, Information Commissioner