For Publication

Bedfordshire Fire and Rescue Authority
Corporate Services Policy and Challenge Group
21 June 2018
Item No. 12

REPORT AUTHOR: **BOROUGH COMMANDER NORTH**

SUBJECT: **GENERAL DATA PROTECTION REGULATIONS**

For further information on this Report contact: Borough Commander North Darren Cook

Tel No: 01234 845010

Background Papers: None

Implications (tick ✓):

LEGAL	✓		FINANCIAL	
HUMAN RESOURCES			EQUALITY IMPACT	
ENVIRONMENTAL			POLICY	✓
CORPORATE RISK	Known	✓	CORE BRIEF	
	New		OTHER (please specify)	

Any implications affecting this report are noted at the end of the report.

PURPOSE:

To update Corporate Services Policy and Challenge Group on the work being undertaken by the Service to meet the requirements of the General Data Protection Regulations.

RECOMMENDATION:

That Members note the contents of the report.

---

1. Introduction

1.1 The General Data Protection Regulations (GDPR) is the biggest change to data protection law in over 20 years. The regulation is EU law and came into force automatically on 25 May 2018. Notwithstanding some uncertainty following the Brexit decision, compliance with the GDPR will be required despite the decision for the UK to leave the EU.

2. Background

2.1 Whilst the fundamental principles of data protection will remain largely unchanged, the new GDPR laws include a number of new approaches and concepts, and will see the Data Protection Act 1998 repealed and replaced with a more detailed regime. The GDPR places increased demands on data controllers which Bedfordshire Fire and Rescue Service (BFRS) is one, requiring them to evidence everything from the legal basis for processing to the sharing of personal information and mandates that they evidence compliance.

2.2 Data protection compliance will become a more significant issue for BFRS. Sanctions on data controllers include potential financial sanctions for non-compliance, which can result in a maximum fine of up to 10 million euros with a fine of up to 20 million euros for a data breach.

2.2 To ensure that BFRS will be in a position to comply with the new data protection laws including the significant and necessary changes to processes, systems, policies, guidance, staff training etc. an intensive work programme has been put in place from information from an internal gap analysis by RSM the Services' internal auditor.

3. What is new under GDPR?

3.1 While the GDPR has many similarities to the Data Protection Act (DPA) at its core it addresses the processing of personal data in a digital age, imposing new obligations on controllers and data processors. It addresses the rights individuals have over the use of their personal information impacting people, processes and technology across all functions of the Service.

3.2 A key change requires organisations to be able to demonstrate how in each case it has complied with GDPR requirements as well as showing compliance through existence of policies and procedures and staff training. It requires accountability at Principal Officer level, evidencing a 'whole system' ethos in the way the organisation protects, governs and understands its data.

4. Work being undertaken to implement GDPR

4.1 GDPR briefing sessions have been carried out at a Management Briefing Day in February to raise awareness and GDPR is reported monthly at the Corporate Management Team meeting (CMT). Staff training is in the process of being finalised with an external provider to cover the requirements of an Information Governance structure, Senior Information Risk Owner (SIRO), Accounting Officer (AO) and Information Asset Owners (IAO).

4.2 A cross-departmental project team reporting to the ACO (HR&OD) - who is the Senior Information Risk Owner (SIRO) for BFRS - been set up to enable to BFRS to meet its obligations under the GDPR. The project team covers work streams in the following areas – Policy and Governance, Data Subject Rights, Communications, Training, Information Collection & Sharing, ICT, Incident Breach Management and Records Management.

4.3 A project plan to map, drive and take action to ensure delivery of each component of the project has been drawn up following an internal gap analysis undertaken by RSM; our internal auditors. Work has commenced to improve understanding on what personal information BFRS holds by contacting Information Asset Owners (Functional Heads of department) to facilitate an information audit to capture a 'what we have now' baseline.

4.4 The action plan provided by RSM contains 10 Service-wide recommendations that need to be completed to ensure compliance with GDPR. A further 26 departmental actions have been identified that will be tracked against progress by the Organisational Assurance Manager. These actions are made up of 17 High, 8 Medium and 1 Low priority.

4.5 GDPR has been placed on the BFRS Corporate Risk Register held and managed by the Head of Service Development and Assurance (HSDA). BFRS have appointed the Data Protection Officer (DPO) to the Head of ICT with support from Business Information Manager (BIM) and Service Assurance Manager (SAM).

4.6 BFRS has completed 22 data processing registers. These registers record where we hold personal data and what processes BFRS have in place to ensure the security of the data. The data registers are dynamic documents and will be reviewed annually by the department responsible for the system to document further changes, such as company take overs, servers moving to the EU or compliance with ISO 27001 being reached. The audit will be carried out by the HSDA to ensure updates and reviews have taken place and have been recorded.

4.7 26 policies have been identified as requiring a review and have been prioritised as high. This is a significant amount of work, which is in progress already and will need to cover areas such as:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- The right not to be subject to automated decision-making, including profiling.

5. Governance

5.1 Work will continue to complete the outstanding actions in the plan and this will be reported to the SIRO and CMT monthly.

6. Risk

6.1 The legal implications are incorporated within the report.

BOROUGH COMMANDER NORTH DARREN COOK