TYNE AND WEAR FIRE AND RESCUE AUTHORITY **Item No 7**

MEETING: 19 MARCH 2018

SUBJECT: GENERAL DATA PROTECTION REGULATION (GDPR) IMPLEMENTATION

JOINT REPORT OF THE CHIEF FIRE OFFICER/CHIEF EXECTIVE (THE CLERK TO THE AUTHORITY) THE STRATEGIC FINANCE OFFICER AND THE PERSONNEL ADVISOR TO THE AUTHORITY

1 INTRODUCTION

1.1 The purpose of this report is to inform Members of upcoming changes to legislation in relation to data protection and the work that is being carried out to ensure compliance with these new regulations.

1.2 The current Data Protection Act 1998 will be replaced by the European Union's General Data Protection Regulation (GDPR) on 25 May 2018. The new act will be reflective of how modern society collects and stores data, introducing Special Categories such as social media and the collection of genetic and biometric data.

1.3 The UK Information Commissioners Office (ICO) has stated their intention to align UK data protection laws to GDPR after exit from the EU, which is tentatively scheduled for 2019.

1.4 The way the Authority collects and processes data will change. Under GDPR, there will be additional steps we have to take before we collect and process personal data.

1.5 There will be a need for us to explain our lawful basis for processing personal data, how long we keep the data and explain to the data subject the process for having their data removed.

2 BACKGROUND

2.1 The GDPR is the biggest revision of global privacy law for over 20 years. It will come into effect on 25 May 2018 and enforcement of the regulations is immediate from that date.

2.2 The cost implications for non-compliance are set at significantly higher levels than the current Data Protection Act (DPA). The current levels are set to a maximum level of £500,000, under GDPR the maximum penalties for non-

compliance or data breaches are EUR 20 million or 4% of global turnover, equivalent to £17 million.

2.3 Reputational damage would also be significant as a result of non-compliance. Breaches of data must be reported to the ICO within 72 hours. One of the post-breach recommendations from the ICO is to issue press releases containing details of the breach to ensure that all affected by a data breach are informed.

2.4 GDPR is based upon the same principles of the existing Data Protection Act; however, it introduces new rights for data subjects (identified or identifiable individuals) such as the right to erasure or restriction of the use of their personal data. It also places new demands on organisations, for example designating a Data Protection Officer (DPO) and formally assessing Data Protection Impacts.

2.5 Under GDPR breach notifications will become mandatory where a breach is likely to result in a risk to the rights and freedoms of individuals. This must be reported to the Information Commissioners Office within 72 hours. The organisation would also need to notify data subjects without delay if their personal data has been breached.

2.6 GDPR will bring in special protection for children's (the age of 16 under GDPR) personal data, particularly in social media platforms. Consent for children's data to be collected by the organisation must come from the parent or guardian in order to process the data lawfully. Any wording aimed at the collection of a child's data must be worded in a manner which is easily understandable to the child.

3 PROGRESS STATEMENT

3.1 In order to ensure compliance with the new regulation a project board has been established to cover the key areas of Policy and Procedure, technical requirements, learning and development and internal data audit. The project remains on schedule for implementation by 25 May 2018.

3.2 Progress to date includes the completion of internal self-assessments covering all functions. These comprehensive self-assessments identify personal data that is handled, stored and transferred internally and externally. They will assist in ensuring compliance with the new regulation remains on schedule.

3.3 Policies and Procedures are now to be reviewed to ensure alignment with GDPR where relevant. A breach policy is in development to ensure effective recording, reporting and rectification of breaches, should they occur.

3.4 In order to meet the technical needs of GDPR, the technical work stream of the project is currently delivering two new systems:

- CoreHR – this will move our HR data into a GDPR compliant system
- Office 365 – this will form the foundation of our ability to manage, monitor and maintain unstructured data (such as email, documents etc.) within GDPR compliance. This system will form the basis of new ways of working to support privacy of data over the coming months.

3.5 Gap analysis is continuing to take place around other supporting ICT systems and a roadmap is being formed as to what interventions, if any, are needed to maximise GDPR compliance throughout the Authority.

3.6 A Service-wide communications strategy is in development to ensure all members of staff are aware of the legislative changes and the impact it has on their roles. This will launch on Monday 26th February 2018 (3 months to compliance) and include:

- CFO bulletins
- A dedicated Intranet section
- 'Countdown to compliance' clock
- Poster campaign across all sites.

3.7 GDPR does have some financial implications, particularly the requirement for specific DPOs. Training for this role was sourced from existing budget and was initially quoted at £2000 per delegate. This was reduced to £1400 per delegate achieving a cost saving of £600 per delegate through the collaborative approach adopted when arranging the training.

3.8 The Authority currently has an E-Learning Data Protection Act package available to all staff via Redkite. The provider has reviewed and updated the content to ensure GDPR compliance. This is scheduled for roll out on 1st April 2018.

3.9 Members of the GDPR board are also utilising a free consultation day with Aristi Information Risk Management & Security Consultants, to carry out a 'GDPR readiness assessment' to assess our current position and detail areas where future action will be required.

3.10 Board members have met with the Principle Auditor of Sunderland City Council to commence the audit process. This process will ensure we are able to demonstrate compliance once the regulations are implemented.

3.11 Next steps:

- Senior Information Risk Officer (SIRO) training – 27 April 2018
- Service-wide roll out GDPR E-Learning package, including exam

- Collation and action of internal self-assessments to support compliance within the timescales
- Review of Information Asset Register (IAR) with support and training for Information Asset Owners (IAOs)
- Further embedding and awareness raising of GDPR at Service Delivery training days.

4 RISK MANAGEMENT

4.1 A risk register has been created to ensure that the risk to the Authority has been minimised as far as practicable. The register has considered an appropriate balance between risk and control, the realisation of efficiencies, the most appropriate use of limited resources and a comprehensive evaluation of the benefits. The register is reviewed and amended regularly at monthly GDPR board meetings.

5 FINANCIAL IMPLICATIONS

5.1 TWFRS Strategic Finance Manager has been consulted on the project for advice and guidance when required.

5.2 A requirement of the GDPR is that the Authority must maintain a separate budget for GDPR. This has been observed and an additional modest sum has been included to recognise the impact of GDPR for the Authority. This will be kept under review to ensure it is adequate and appropriate.

6 EQUALITY AND FAIRNESS IMPLICATIONS

6.1 The first principle of the GDPR is that data must be processed lawfully, fairly and transparently. This allows individuals to have greater ownership of who has access to their personal data, allowing them to ensure that data is held lawfully or with consent and also allows individuals to withdraw their consent at any time.

7 HEALTH AND SAFETY IMPLICATIONS

7.1 There are no health and safety implications in respect of this report.

8 RECOMMENDATIONS

8.1 The Authority is recommended to:

a) Note the contents of this report

b) Receive further reports as appropriate.

BACKGROUND PAPERS

The under mentioned Background Papers refer to the subject matter of the above report:

September 2017 ELT Paper ‘General Data Protection Regulations (GDPR)’.