*Mae'r ddogfen yma ar gael yn Gymraeg* **Agenda Item 8**

| | |
|---|---|
| Report to | **Executive Panel** |
| Date | **16/07/2018** |
| Lead Officer | **Shân Morris, Assistant Chief Officer (Corporate Policy and Planning)** |
| Contact Officer | **Brian Mottershead, Data Protection Officer** |
| Subject | **European Union General Data Protection Regulation and UK Data Protection Act 2018** |

## PURPOSE OF REPORT

1 To inform members of progress made in relation to North Wales Fire and Rescue Service (the Service)'s compliance with the European Union (EU) General Data Protection Regulation (GDPR) and the United Kingdom (UK) Data Protection Act 2018.

## EXECUTIVE SUMMARY

2 Progress continues towards ensuring the Authority's full compliance with the new data protection legislation. As more guidance is issued by the Information Commissioner's Office, so work is completed to amend or introduce new processes and procedures.

## RECOMMENDATION

3 That members note and approve the progress made by the Service towards complying with the new data protection legislation.

## BACKGROUND

4 The GDPR came into effect on 25 May 2018. This regulation is intended to strengthen and unify data protection for individuals within the EU, and also addresses the export of personal data outside the EU.

5 The UK Data Protection Act 2018 received Royal Assent on 23 May 2018. This Act is intended to modernise data protection laws in the UK to meet the needs of an increasingly digital economy and society. It provides a legal framework for data protection, implements GDPR standards across all general data processing and ensures that the UK continues to have appropriate data protection legislation in place after it leaves the EU.

6 The new legislation requires organisations that process personal data to ensure that they use that data: fairly, lawfully and transparently; for specified, explicit purposes; and in a way that is adequate, relevant and limited to only what is necessary.

7 The new legislation also requires those organisations to ensure that the personal data that they process: is accurate and, where necessary, kept up-to-date; is kept for no longer than is necessary; and is handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

8 A report to the Executive Panel meeting in February 2018 highlighted some of the significant new requirements of the GDPR and the progress that the Service was making towards ensuring compliance with the GDPR.

9 Those significant new requirements of the GDPR related to:

a. the need for public authorities to have a Data Protection Officer (DPO) who reports to the highest management level of the organisation, operates independently and is provided with adequate resources in order to meet their GDPR obligations;
b. the requirement to report certain breaches of personal data to the Information Commissioner's Office within 72 hours of becoming aware of them, or risk a fine of up to €10 million or 2% of turnover;
c. a general obligation to integrate data protection as an intrinsic aspect of processing activities - data protection by design and by default.

10 Members were also informed that the Service had established a project team to ensure delivery of a GDPR Implementation Plan, with regular reporting and monitoring of progress to senior management.

**INFORMATION**

11 Since the previous report to members, the Service has completed a number of actions to ensure compliance with the requirements of the GDPR. However, further actions remain as expanded and new guidance continues to be issued by the Information Commissioner's Office. Members may also wish to note that the European Data Protection Board has recently consulted on establishing voluntary certification mechanisms for organisations to demonstrate their compliance with the GDPR.

12 Within the Service, work continues on ensuring full compliance with the GDPR. Progress made since February 2018 includes:

- **Appointing a DPO** - Brian Mottershead, the Project Manager for the GDPR Implementation Project, was appointed on an interim basis to the role of Data Protection Officer (DPO) with effect from 25th May 2018.

- **Training –** A GDPR e-learning package has been identified and is currently being adapted for delivery to all Service staff.

- **Issuing privacy notices** - Following the Information Commissioner's advice to take a 'layered approach' to providing people with privacy information, an overarching privacy notice has been placed on the Service's website, together with specific privacy notices for individual activities such as conducting Safe and Well Checks. Structuring privacy notices in this way will allow for additional ones to be issued when required, and should help to simplify the task of reviewing them to ensure that they remain up-to-date.

- **Information Asset Mapping** - Under the GDPR, data processors are required to maintain a record of their data processing activities, covering areas such as why they process the data, who they share it with, and how long they retain it. Keeping an Information Asset Register is a way of recording what information is held, where it is and what it is used for. It also makes it easier to comply with other aspects of the GDPR such as making sure that the information held about people is accurate and secure.
  A Service-wide Information Asset Register has now been compiled, and is in the process of being checked for accuracy and completeness.

- **Contracts**: Whenever a data controller uses a data processor there should be a contract in place setting out both parties' responsibilities and liabilities. The GDPR sets out what needs to be included in contracts involving the sharing of personal data. The European Commission or the Information Commissioner's Office may in future provide standard contract clauses, but have not done so yet. However, the Crown Commercial Service's comprehensive guidance on achieving GDPR compliance in relation to contracts has been widely adopted across the public sector.
  All contracts entered into by either the Service or the Authority that involve the sharing of personal data with external organisations are currently being reviewed for GDPR compliance.

- **Policies and procedures**: The legislation requires that data protection is integrated into all processing activities and business practices 'by design' rather than as an adjunct.
  All Service policies and procedures are being reviewed for GDPR compliance.

- **Accessing personal data**: Individuals have a right to access their own personal data and the Service must respond to a person's 'Subject Access Request' within one month.
  A process has been established to help ensure that the Service can retrieve the relevant information and provide only the information that the individual has a legitimate right to access, without delay and by the appropriate deadline.

- **Data breaches**: the GDPR places a duty on organisations to report certain types of personal data breach to the Information Commissioner's Office within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, organisations must also inform those individuals without undue delay.
  A process has been developed to enable the Service to respond appropriately and promptly to potential breaches of personal data.

13 The GDPR Implementation Project Team continues to meet to monitor progress and identify necessary actions, and regular reports continue to be provided to the Service's Executive Group.

**IMPLICATIONS**

| | |
|---|---|
| Wellbeing Objectives | None identified. |
| Budget | Funding for new statutory role of DPO. Possible expenditure on appropriate technical measures to facilitate compliance. |
| Legal | As a public authority, NWFRA is required to comply with the new legislation. |
| Staffing | Existing staff form the implementation project team. New DPO role introduced. |
| Equalities/Human Rights/Welsh Language | None identified. |
| Risks | Risk of incurring fines and reputational damage if the Authority fails to comply with the requirements of the data protection legislation. |