Report to:	Governance and Audit Committee
Date:	29 March 2018
Subject:	**General Data Protection Regulation Progress**
Director(s):	Angela Taylor, Director, Resources
Author(s):	Rebecca Brookes

1 Purpose of this report

1.1 To provide details of the key changes made by the General Data Protection Regulation (GDPR) to the current data protection framework and to provide a progress report on the readiness of the West Yorkshire Combined Authority for implementation of the GDPR.

2 Information

Background

2.1 The General Data Protection Regulation (GDPR) will come into force on 25 May 2018, it will have direct effect across all EU member states and will bring significant changes to the law on data protection.

2.2 The aim of the new legislation is to modernise the law on data protection to ensure it is effective in the years to come and to ensure consistency across EU member states. It applies to all business and organisations that process personal data including the Combined Authority.

Key changes to the data protection legal framework

2.3 The key changes arising out of the new legislation are:

- An obligation to appoint a Data Protection Officer who is involved in all issues relating to the protection of personal data, is adequately resourced, permitted to act independently without instruction, is the organisation's point of contact for the Information Commissioner and data subjects and reports directly to the highest level of management.
- New specific obligations to "demonstrate compliance" and "maintain records" signifying a "whole systems" approach towards compliance.

- Changes to the lawful bases for processing personal data (the justifications for processing data), including higher standards for relying on data subject consent for processing and the recording of consent.
- New “special categories” of personal data, previous known as categories of “sensitive” personal data including genetic and biometric data categories.
- Stricter requirements for the giving of privacy notices including communicating the processing of children’s personal data.
- Changes to the rights of data subjects including the abolition of the £10 subject access fee, restricting the time for compliance with requests to 1 month and rights in respect of the deletion and restriction of data processing, data rectification, data quality, data portability and automated decision making.
- Mandatory requirements to complete Data Protection Impact Assessments for high risk processing activities, consider the use of technical measures including encryption, anonymisation and pseudonymisation and an obligation to consult the ICO before carrying out high risk processing.
- Introduction of the concepts of “data protection by design” and “data protection by default”. “Data protection by design” requires taking data protection risks into account throughout the design of a new process or service and taking appropriate measures to address any risks to the rights of data subjects. “Data Protection by default” requires ensuring mechanisms are in place within the organisation to ensure that by default, only personal data necessary for each specific purpose are processed (“data minimisation”), data is stored no longer than is necessary and access is restricted to that necessary for each purpose.
- Specific requirements for data processing and contractual arrangements including ensuring that data processors offer sufficient guarantees of compliance with the GDPR, the use of mandatory clauses within contracts and giving clear instructions to processors on data processing activities.
- A new requirement to report data breaches that result in a risk to individuals’ rights and freedoms to the ICO and within 72 hours of the organisation becoming aware of the breach.
- A new requirement to notify data subjects of data breaches without undue delay where there is a high risk to the individuals’ rights and freedoms.
- Increased enforcement powers for the Information Commissioner including the power to impose fines of up to 20 million Euros (approx. £17 million) or 4% of annual turnover whichever is greater (raised from the current £500,000 maximum fine).

Action Taken

2.4 The report provided to Governance and Audit Committee on 25 January 2018 gave an update on the preparatory work already taken by officers.

2.5 Since that date, the author of this report and Data Protection Officer (DPO) has joined the organisation, analysed progress taken to date, further developed the action plan that was developed following the information audit and has produced a further iteration of the specific GDPR implementation plan.

2.6 The GDPR implementation plan is divided into 6 work streams comprising of individual tasks, full details of which can be found at Appendix 1:

Governance and Reporting

2.7 A significant amount of work has already been undertaken on this work stream and preparations are almost complete. Prior to 25 May the reporting arrangements of the DPO will be finalised.

Awareness and Training

2.8 Talks are underway with the Combined Authority's current training provider to ensure that the data protection e-learning platform can be updated for GDPR compliance. Staff will be required to complete the training on an annual basis and arrangements are being put in place to ensure that staff complete the training prior to accessing data held by the Combined Authority.

2.9 Further awareness sessions are being held by the DPO and Information Governance Officer (IGO) to prepare staff for the changes that GDPR brings, embed information governance throughout the organisation and to engage staff in the implementation project plan.

2.10 The dedicated Information Governance intranet mini –site has been launched.

2.11 An internal communications strategy is being developed to communicate key messages to staff regarding GDPR and their involvement in the implementation project.

Records and Audits

2.12 Further work is required by Information Asset Owners (IAOs) to fully populate the Information Asset Register, map data flows throughout the organisation and address compliance gaps. An electronic information audit questionnaire is being developed to streamline this task which will be shortly rolled out for completion by IAOs within April. This will enable compliance gaps to be assessed and addressed before the implementation date.

2.13 A process of reviewing and destroying information which the organisation should no longer hold is underway with some records having been transferred to the West Yorkshire Archive, however further work is required and the scale of this task should not be underestimated. Dedicated resource will be required in order to complete the review. This work is required not only to support the GDPR implementation project but also to support the wider organisational transformation programme and the corporate technology strategy.

Policies and procedures

2.14 A suite of information governance policies are already in place and work has commenced on reviewing all of the organisation's policies for GDPR implications and compliance.

2.15 A new data and systems security incident policy has been put in place to facilitate a quick and co-ordinated response to any data incidents and enable compliance with the new breach notification timescales.

Projects and Initiatives

2.16 Legal and procurement officers are in the process of updating the Combined Authority's standard contract clauses and tender documentation to ensure that the Combined Authority complies with its obligations in respect of data processors for all new arrangements.

2.17 A review will be carried out of all existing data processor arrangements to ensure that our processors offer sufficient guarantees of compliance and to vary contracts to meet the requirements of the GDPR.

Security and Systems

2.18 A systems audit will be carried out across all the Combined Authority's systems and data storage facilities to check for compliance with GDPR, identify any compliance gaps in those systems and put measures in place to address or mitigate any risks arising.

2.19 Much of the work arising out of this work stream ties into the Combined Authority's corporate technology strategy and the wider one organisation programme.

Progress Report

2.20 A progress report monitoring each of the work streams and progress of individual task can be found at Appendix 2.

2.21 A significant amount of work has already been undertaken in preparation for the new regulations with those tasks marked as green either complete or due to be completed imminently. Work on those tasks marked as amber is well under way, however further work is required between now and 25th May to ensure that those tasks are completed on time.

2.22 There are two tasks that are marked as red within the progress report which present a higher risk to the Authority. The first of these is records management. Historically the organisation has relied on papers records and the use of network drives for record storage across many services. Whilst this method of storage in itself does not result in non-compliance with the legislative framework, it does place heavy reliance on the manual control of

records and application of retention periods. As part of the Corporate Technology Strategy work will be carried out to redesign network folders, introduce data management and information rights management infrastructure, and to implement new and refreshed corporate systems. This will address many of the challenges facing the Authority in the use of current data storage methods. In the meantime, and prior to 25th May, the author together with the Authority's Information Governance Officer will work with IAOs to put in place a records management strategy for each service area including a timeline for reviewing existing records.

2.23 The second area marked as a risk to the Authority is the potential upgrade or replacement of non-compliant systems and the review of network security. A plan is in place to review all existing systems for compliance by 25th May and where possible put in place measures to mitigate any risks to an acceptable level. Beyond 25th May many of the Authority's systems are planned for upgrade or replacement as part of the Corporate Technology Strategy and compliance with GDPR will form part of the specification for those systems. Priority one on the Corporate Technology Strategy is Security and Compliance which includes making improvements to the Authority's defences, introducing government secure email for sensitive information and obtaining Public Services Network accreditation for external partner integration, this will deliver confidence that the Authority's systems and data are not compromised by malicious threats.

2.24 On the whole the Authority is in an advanced state of readiness for implementation of GDPR by 25th May. The month of April will see a significant amount of further work throughout the Authority to progress and complete those tasks that remain ongoing. Where risks do exist, plans are in place to manage and mitigate those risks as set out above.

3 Financial Implications

3.1 Additional resource will be required to ensure GDPR compliance, in particular for GDPR compliant training, records management and ICT security and systems. Consideration is currently being given to how best to meet those resource requirements.

4 Legal Implications

4.1 Non-compliance with the GDPR could potentially lead to personal data being processed unlawfully giving rise claims against the organisation, reputational damage and enforcement action by the Information Commissioner in the form of external audits, corrective action, or financial penalties.

5 Staffing Implications

5.1 There are no staffing implications directly arising from this report.

6 External Consultees

6.1 No external consultations have been undertaken.

7 Recommendations

7.1 That Governance and Audit Committee notes the key changes arising from GDPR, the approach the Combined Authority has developed to ensure compliance and readiness prior to implementation on 25 May 2018 and the progress made to date and provide any feedback on this.

8 Background Documents

None.

9 Appendices

Appendix 1 - GDPR Implementation Plan

Appendix 2 - GDPR Progress Report