Report to:	West Yorkshire Combined Authority
Date:	10 May 2018
Subject:	**General Data Protection Regulation**
Director:	Angela Taylor, Director of Resources
Author(s):	Rebecca Brookes

Is this a key decision?	☐ Yes ☒ No
Is the decision eligible for call-in by Scrutiny?	☐ Yes ☒ No
Does the report contain confidential or exempt information or appendices?	☐ Yes ☒ No
If relevant, state paragraph number of Schedule 12A, Local Government Act 1972, Part 1:	

1 Purpose of this report

1.1 To provide details on the approach that West Yorkshire Combined Authority has developed to ensure compliance with the General Data Protection Regulation.

2 Information

The new legislation

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. It applies to all businesses and organisations that process personal data including the Combined Authority.

2.2 Although the GDPR builds on existing data protection principles there is a considerable level of change in practice, including:

- An obligation to appoint a Data Protection Officer
- New obligations to maintain records and demonstrate compliance

- Changes to the way an authority obtains and records consent
- Stricter requirements for the giving of privacy notices
- Increased data subject rights
- Mandatory data protection impact assessments
- Specific contractual clauses for data processing arrangements
- A requirement to report data breaches within 72 hours
- A new requirement to notify data subjects of data breaches in certain circumstances
- Increased fining 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).

Level of assurance

2.3 The Information Commissioner assesses the arrangements that an organisation has for compliance with data protection legislation and adherence to those arrangement by completing audits and offering an overall 'assurance rating of 'high', 'reasonable', 'limited' or 'very limited'.

2.4 On the whole the Combined Authority considers it is in an advanced state of readiness for implementation of the GDPR and work is ongoing to ensure that where possible outstanding tasks are completed by 25 May 2018. Where risks exist, plans are in place to manage and mitigate those risks.

2.5 The Combined Authority is aiming to offer a 'reasonable' level of assurance by 25 May 2018 and working towards a 'high' level of assurance in the longer term once the records management strategy and corporate technology strategies have been delivered.

2.6 It is proposed that updates on GDPR status are provided to each meeting of the Combined Authority and Governance and Audit Committee as part of the regular risk reporting arrangements. It is further proposed that the Overview and Scrutiny Committee consider whether a review of GDPR arrangements should form part of their programme for the year.

Action taken and progress report

2.7 An Information Governance (IG) audit was undertaken in June/July 2017, concluding in recommendations for change and improvement. The recommendations have formed the basis of an IG project plan which has subsequently been developed into a specific GDPR implementation plan. Further details of the action taken as part of those plans is detailed in **Appendix 1**.

2.8 A significant amount of work has already been undertaken in preparation for the new regulation and work is underway throughout the organisation to complete outstanding tasks by 25 May 2018. However, there are two work streams that will continue beyond 25 May 2018, namely records management and ICT security and systems.

2.9 With regards to records management, work will be carried out as part of the Combined Authority's Corporate Technology Strategy to redesign network folders, introduce data management and information rights management infrastructure, and to implement new and refreshed corporate systems. In the meantime, and prior to 25 May 2018, key officers will work with information asset owners to ensure that records are held in line with retention periods.

2.10 With regards to ICT systems, many of the Combined Authority's systems are planned for upgrade or replacement as part of the Corporate Technology Strategy and GDPR compliance will be a requirement for those systems. The first priority on the Corporate Technology Strategy is Security and Compliance which includes making improvements to the Combined Authority's defences, introducing government secure email for sensitive information and obtaining Public Services Network accreditation for external partner integration. In the meantime key officers are working with information asset owners to ensure that current systems are used in line with the GDPR.

3 Inclusive Growth Implications

3.1 There are no inclusive growth implications arising directly from this report.

4 Financial Implications

4.1 None arising directly from this report as work is being undertaken using existing resource. Consideration will be given to the case for any further investment for example to improve legacy systems or to further the work on records management.

5 Legal Implications

5.1 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.

6 Staffing Implications

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

7 External Consultees

7.1 No external consultations have been undertaken.

8 Recommendations

8.1 That the Combined Authority notes the approach developed to ensure compliance with the GDPR and the progress made to date and provide any feedback on this.

9 Background Documents

None.

10 Appendices

Appendix 1 – GDPR Implementation Plan