Report to:	**Audit Best Value and Community Services Scrutiny Committee**
Date of meeting:	**22 March 2018**
By:	**Chief Operating Officer**
Title:	**General Data Protection Regulation (GDPR) Preparedness**
Purpose:	**Update on the Council's preparedness for new data protection legislation (GDPR)**

RECOMMENDATIONS

1) The Committee are asked to note the contents of this report

---

1 Background

1.1 New data protection legislation is due to come into force in May 2018 and an 'Action Plan' is being implemented to deliver required change. A cross-departmental steering group, chaired by the Information Manager, has been created to support delivery of the action plan and sub groups established to focus on specific work-streams within the plan.

1.2 This report summarises requirements of the new legislation, associated risks and progress to date in preparing for the change.

2 Supporting information

2.1 The General Data Protection Regulation (GDPR) is European legislation that will apply in the UK from 25th May 2018. The UK is additionally looking to replace the current Data Protection Act (1998) and a Bill is currently being considered by parliament. This Bill includes requirements of the GDPR (and applicable derogations) and the Law Enforcement Directive. The East Sussex County Council (ESCC) GDPR Action Plan is being updated, where information on the new Data Protection Act is known, to ensure the Council is able to respond to the wider legislation.

2.2 Failure to reach an adequate level of compliance with the new legislation risks reputational damage and significant fines. The monetary penalties that the Information Commissioner's Office (ICO) can administer rise from a maximum of £500,000, under the current legislation, to €20 million (or 4% of turnover – whichever is greatest) under GDPR.

2.3 Whilst the GDPR (and associated legislation) mirrors current law to a large degree, it requires organisations to put additional safeguards in place to meet privacy obligations and enhances the rights of individuals where personal data is processed. **A summary of the Council's response to these requirements can be found in Appendix 1.**

2.4 ESCC's preparedness for GDPR/Data Protection Law is the subject of a current internal audit exercise. The report and findings are due by 31st March 2018 and will be reported in the Audit report to this committee at its meeting on 13th July 2018.

2.5 In order to ensure consistency of approach in response to the new legislation, ESCC is working closely partners including Health, Orbis Councils and Sussex Police.

2.6 One key requirement of the GDPR is the appointment of a Data Protection Officer (DPO). The Orbis partnership is currently working to appoint a DPO in advance of May 2018.

3. Conclusion

3.1 ESCC has made good progress in preparing for the change in Data Protection legislation and whilst much work is still to be done, all required elements (summarised in Appendix 1) are being addressed to enable requirements for compliance to be in place by 25th May 2018.

KEVIN FOSTER
Chief Operating Officer

Contact Officer: Heidi Judd (Information Manager)
Tel. No. 01273 482184
Email: heidi.judd@eastsussex.gov.uk

Appendix 1 - GDPR Progress Dashboard

Mar 18

Privacy Impact Assessments (PIA)

Progress

- PIA Template and Guidance published on the intranet

Next Steps

- Align corporate Project and Change Management processes with PIA process

Privacy Notices (PN)

Progress

- Draft Privacy Notice guidance/graphics complete
- Privacy Notice template created and web form nearing completion
- Current Privacy Notices – updates nearing completion
- Privacy Notice area created on ESCC website

Lawful Processing

Progress

- Guidance on applicable conditions for processing personal data complete
- Consent guidance nearing completion

Information Asset Register (IAR)

Progress

- IAR Update - in progress
- Personally Identifiable Information (PII) Data Flow Mapping – in progress

Next Steps

- Ongoing maintenance and development plan

Data Subject Requests

Progress

- Rights review complete
- Guidance for customers complete
- Guidance for customers nearing completion
- Gap analysis – IT systems review: ability to meet Data Subject Rights – in progress
- Data Subject Rights request process agreed

Procurement and Contracts

Progress

- New contract T&Cs in place
- Contract variations being prepared
- Procurement checklist nearing completion

Policy/Governance Review

Progress

- Gap analysis – complete
- Policy update – nearing completion

Next Steps

- Decision log creation
- Process change

Breach handling

Next Steps

- Review and update procedures (if required)
- 72 hour breach response – 'rapid response team'

Communications Plan

Progress

- Communications plan and comms. team support in place
- High level cross-council awareness – intranet content, yammer, CMT Brief and posters
- Targeted departmental and specific service area communications – in progress
- ESCC Website content update including GDPR guidance for Data Subjects - nearing completion