Report to:	**Pension Board**
Date:	**8 February 2018**
By:	**Chief Operating Officer**
Title of report:	**Preparing for General Data Protection Regulation (GDPR)**
Purpose of report:	**To outline progress in preparing for new data protection legislation**

RECOMMENDATION

The Board is recommended to consider and comment on the report.

1. Background

The General Date Protection Regulation (GDPR) is due to come into force in May 2018. This report summarises progress to date and highlights future areas of activity in Pensions Administration to ensure compliance with the new legislation.

2. Work-stream Summary

As this new legislation affects all aspects of East Sussex County Council, a County wide steering group, led by the Information Manager, has been established to plan and prepare using an action plan. This plan is also being used across the Orbis partnership and with other partner organisations such as Health and Sussex Police.

Appendix 1 provides an overview of progress as at November 2017.

3. UK Data Protection Bill

A Bill looking to replace the current Data Protection Act (1998) is currently being considered by Parliament. This Bill includes GDPR, specific derogations within GDPR and the Law Enforcement Directive. The ESCC GDPR Action Plan is being updated to ensure the Council is able to respond to the wider legislation (it is not currently clear when this legislation will come into force).

4. Pensions Administration activity

The action plan has a number of key workstreams which can be summarised below along with the current position and actions which directly affect Pensions Administration activity.

1. **Maintain Records of Data Processing** = ESCC has an Information Asset Register (including Pensions data) that will be used for this purpose. A dedicated resource is being employed to update it and add relevant information required under GDPR.
2. **Data Security Measures** = a systems gap analysis (including Pension Scheme systems and document storage) is being undertaken across ESCC. Risk assessment on Altair including the online portal is scheduled.
3. **Update Service Provider Contracts** = Orbis Public Law and Orbis Procurement will introduce new procurement processes and contract terms and conditions. Existing contracts will be subject to variation – letters are being prepared and disseminated on behalf of ESCC.
4. **Revise and Update Privacy Notices and Consider Whether Member Consent Is Required** = Privacy notices are to be updated. Pensions: consent will not be widely relied on - alternative legal conditions for processing have been identified. Where consent is used (in niche cases) explicit consent will be obtained and recorded.
5. **Breach management process** = already in place.

6. **Privacy Impact Assessment (PIA)** = Pensions PIA in progress, currently identified areas of focus:

   ACTION 1: Privacy Notice; Employer has to inform employee that they will be automatically enrolled. Then pensions team to send out notice - this is what we collect and why (link to pensions fund website). A general statement is being prepared by the Pensions Team. A link to this Notice will also be included in standard correspondence to existing members.

   ACTION 2: Data storage limitation vs data minimisation - look at possible ways to filter records if required.

   ACTION 3: Risk assessment on Altair is scheduled.

KEVIN FOSTER
Chief Operating Officer

Contact Officer: Heidi Judd, Information Manager 01273 482184

Appendix 1 - GDPR Progress Dashboard

Nov 17

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

Next Steps

- Privacy notice audit and creation of privacy notice register
- Generic and specific/tailored PNs to be published on ESCC Website

Lawful Processing

Progress

- Guidance on applicable conditions for processing personal data in progress
- Review of use of Consent condition

Next Steps

- Publish guidance on intranet

Information Asset Register (IAR)

Progress

- IAR Update - in progress

Next Steps

- Personally Identifiable Information (PII) Data Flow Mapping
- Ongoing maintenance and development plan

Data Subject Requests

Progress

- Rights review complete
- Guidance for customers – in progress

Next Steps

- Gap analysis – IT systems review: ability to meet Data Subject Rights
- Process change

Procurement and Contracts

Progress

- New contract T&Cs
- Supplier due diligence guidance
- Contract variation letter templates

Next Steps

- Contract variations
- Procurement checklist

Policy/Governance Review

Progress

- Gap analysis – complete
- Policy update – in progress

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 and posters

Next Steps

- CMT Report and Member engagement
- Targeted departmental and specific service area communications
- Data Subject Rights - website