Report to: **Pension Board**

Date of meeting: **3 August 2017**

By: **Chief Finance Officer**

Title: **General Data Protection Regulation (GDPR)**

Purpose: **This report provides the Board with an update on the General Data Protection Regulation (GDPR), a legal framework proposed by the European Commission**

RECOMMENDATION

The Board is recommended to note the EU's General Data Protection Regulation (GDPR) framework requirements.

---

1. Background

1.1 The EU's General Data Protection Regulation (GDPR) is a legal framework first proposed by the European Commission in January 2012 with the aim of boosting online privacy rights and strengthening the digital economy in the European Union. This was in response to how both globalisation and technological change have impacted how data is collected, stored, shared and transferred.

1.2 The General Data Protection Regulation (GDPR) will come into force in all EU Member States on 25 May 2018. The UK will still be a Member State of the EU on 25 May 2018 and is likely to retain the GDPR following Brexit. The GDPR does not mark a radical departure from the current data protection regime (i.e. in the UK under the Data Protection Act 1998 (DPA)). There are, however, certain key changes that will focus attention in the pensions industry. The GDPR contains key developments that members, employers and the pensions industry will need to grapple with.

2. What are the key changes for Pension Fund under the GDPR?

2.1 Pension schemes necessarily hold and process significant amounts of personal data relating to members. As a matter of good governance, it is important that member data is safeguarded. There is already a legal obligation on LGPS fund Administering Authorities to keep member data secure, but new legislation will have a significant impact on the obligations of Administering Authorities and the potential financial penalties if they get it wrong.

2.2 Some of the key areas covered by GDPR are as follows:

	Key Changes	Description
i	Stricter requirements around consent	The fund must be able to demonstrate that individuals have explicitly consented to the processing of their data. The regulations allow consent to be withdrawn by the individual at any time. So consideration should be given to, for example, whether consent is deemed explicit or given where an individual signs up to being a member of a pension scheme. This includes information about their spouse and dependents and where members have opted out through auto-enrolment.
ii	Privacy notices on use of data	Privacy notices provided to members detailing how their data will be used must now include information such as: • the purpose for which the data processing is intended • the recipients of the personal data • the period which the data will be stored

		• the various rights members have in respect of the information. Any communications must be easy to understand clear and plain language. Consideration will need to be given to what is included in these notices to members.
iii	Right to be forgotten	Members can request the complete erasure of personal data in certain circumstances such as where the data is no longer necessary for the purpose it was collected.
iv	Relevant and necessary	Information must be relevant and not kept for longer than is necessary. Pension schemes will typically keep information for decades and the fund will need to consider whether this is still appropriate, for example where a member has transferred out of a scheme.
v	Data processing contracts	Detailed contracts must be in place between the fund and data processers, such as scheme administrators and other service providers, which will need to comply with GDPR when it comes into force. Fund may need to amend the terms of existing contracts as well as ensuring new contracts will be compliant.
vi	Reporting data breaches	Personal data breaches must be notified to the Information Commissioners Office within 72 hours of having become aware of a breach. The member must also be notified if the breach is likely to result in a high risk to the member.
vii	Data protection impact assessments	Where systems changes are planned and the processing of data is considered 'high risk', an assessment of the impact of the planned processing on the protection of personal data must be carried out.
viii	Increased record keeping obligations	The fund must ensure records are maintained to show how they comply with GDPR.

3. Next steps

3.1 The Pension Fund need to consider how these new requirements apply to our existing arrangements and put a plan in place to ensure that they are compliant by 25 May 2018. This should include considering any information that may be held by members, employers, outsourced providers, and advisors.

3.2 The Head of Pensions will be consulting Business Operations - Orbis, to demonstrate compliance with the GDPR in relation to ESPF and to show in a meaningful way that both the overall governance structure for data protection compliance and the individual policies and procedures relating to data processing are compliant.

4. Conclusion and reasons for recommendations

4.1 The Board is recommended to note the European Union's new General Data Protection Regulation (GDPR), which will be enforced by 25 May 2018.

IAN GUTSELL
Chief Finance Officer

Contact Officer: Ola Owolabi, Head of Pensions
Tel. No. 01273 482017
Email: Ola.Owolabi@eastsussex.gov.uk

Background Documents
None