Croydon Council

REPORT TO:	**Local Pension Board 11 January 2018**
SUBJECT:	**The General Data Protection Regulation**
LEAD OFFICER:	**Nigel Cook, Head of Pensions and Treasury**
CABINET MEMBER	**Councillor Simon Hall Cabinet Member for Finance and Treasury**
WARDS:	**All**
CORPORATE PRIORITY/POLICY CONTEXT: **Sound Financial Management**: this report considers the introduction of additional responsibilities for the administering authorities in respect of data protection.	
FINANCIAL SUMMARY: there are significant fines for non-compliance with these additional regulatory requirements.	
FORWARD PLAN KEY DECISION REFERENCE NO.: N/A	

1 RECOMMENDATIONS

1.1 The Board is asked to note the contents of this report.

2 EXECUTIVE SUMMARY

2.1 This reports sets out the requirements for the Council, as administering authority for the Local Government Pension Scheme, to comply with the General Data Protection Regulation.

3 DETAIL

3.1 The General Data Protection Regulation (GDPR) will have direct effect throughout the EU from 25 May 2018. It applies to all EU member states and provides a single EU legal framework for the processing of individuals' data. The maximum potential fine for breaching the GDPR will be €20 million (or 4% of global turnover if higher). 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 come into force in May 2018 that will have a significant impact on the obligations of Administering Authorities and the potential financial penalties if they get it wrong.

3.2 The government has confirmed that, despite Brexit, the GDPR will be enforceable in the UK from May next year.

3.3 Administering Authorities are responsible for the personal data held by their LGPS funds, meaning the GDPR changes are relevant to them. Administering Authorities must demonstrate compliance with the GDPR in relation to their LGPS fund. Under these Regulations they should be able 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.

3.4 It will become a mandatory requirement for Administering Authorities who employ more than 250 people, or who process sensitive personal data (about members' health or family circumstances), to maintain records of all personal data processing activities. The records may have to be presented to the Information Commissioner's Office (ICO) on demand.

3.5 The GDPR retains the current obligation to have appropriate technical and organisational data security measures in place, but also provides that certain specific measures (such as encryption) should be used "where appropriate". It also requires that processes incorporate "privacy by design and default", i.e. compliance with the GDPR needs to be integrated into all data processing and should be the default setting on all privacy arrangements.

3.6 The GDPR requires new content to be inserted into all service and data sharing agreements that govern the use of personal data. It also imposes direct liability on such service providers for data protection compliance. This will therefore encompass the contractual agreements with Scheduled, Community and Admitted Bodies, auditors (internal and external), the Scheme Actuary, and payroll providers.

3.7 The GDPR requires additional content to be included in all privacy notices regarding how personal data will be used by data controllers. A data controller is any organisation that makes decisions on how personal data is to be processed and for which purposes, so will include the Administering Authorities of an LGPS fund. Data controllers must tell anyone whose personal data they collect what information is held, how it is used, who it may be shared with and what safeguards are in place.

3.8 The GDPR also makes it more difficult to obtain valid consent for the use of personal data – consents must be fully informed, specific, unambiguous and freely given by way of a statement or clear affirmative action by the member. In addition, there is a specific obligation to retain proof of consent.

3.9 The GDPR requires data breaches involving any risk to individuals to be reported to the ICO "without undue delay", and within 72 hours of becoming aware of the breach in any case. The report must contain details of the breach, including the number of individuals affected, the likely consequences and the steps being taken to address/mitigate the breach. Affected individuals must also be notified directly if the breach is a "high risk" to their rights and freedoms.

3.10 As public bodies, Administering Authorities may be required to appoint a DPO. The European data protection authorities recommend that a DPO is appointed

even if an organisation is not required to have one under the GDPR. The DPO is expected to be appropriately qualified and should report directly to the senior management at the authority. The DPO will be the contact person in the organisation for questions related to processing of personal data in respect of the LGPS fund, as well as the rest of the Administering Authority's functions.

3.11 There is a project in place to ensure compliance with GDPR which is led by the Council's Monitoring Officer. For the purposes of GDPR, the Head of Corporate Law (Deputy Monitoring Officer) has been designated as the Council's Data Protection Officer and the project group includes officers from across the organisation and is being supported by our internal audit provider, Mazars.

3.12 The GDPR introduces new rights for individuals, including the right of data portability, the right to restrict processing, the right to object to processing, the right to object to direct marketing and the right to be forgotten – i.e. the right to have one's personal data deleted.

3.13 Data Protection Impact Assessments (DPIAs) must be carried out in relation to all "high risk" processing. This is where there is a high risk to rights and freedoms, for example, extensive profiling of individuals using automated processing or large scale processing of sensitive personal data (e.g. medical information). The European data protection authorities recommend to carry out DPIAs as good practice and to demonstrate accountability for processing personal data. Consultation with the ICO may be required prior to processing in relation to high risk processing in certain circumstances.

4 CONSULTATION

4.1 Officers have fully consulted with the Pension Fund's advisers in preparing this report.

5 FINANCIAL CONSIDERATIONS

5.1 The fines associated with non-compliance with the Regulations are significant.

7 FREEDOM OF INFORMATION/DATA PROTECTION CONSIDERATIONS

7.1 This report does not contain any information which will not be made publically available by being published on the Council's Pension Fund website.

CONTACT OFFICER:

Nigel Cook – Head of Pensions and Treasury
Corporate Resources Department, ext. 62552.