Appointment of Data Protection Officer pursuant to the GDPR

Summary
The General Data Protection Regulation requires all public authorities to appoint a Data Protection Officer by statute. This report proposes the appointment of the Head of Legal Services as the Data Protection Officer.

Portfolio: Transformation
Date Portfolio Holder signed off report: 22 February 2018

Wards Affected: All

Recommendation

The Executive is advised to RESOLVE that the Head of Legal Services be appointed as the Data Protection Officer in accordance with the General Data Protection Regulation.

1. Key Issues

1.1 The General Data Protection Regulation (GDPR) is the new data protection framework for the EU and will apply in the UK from 25 May 2018. It replaces all current data protection legislation, including the Data Protection Act 1998.

1.2 The GDPR regulates how data is processed and sets out a wider definition of personal data than currently. The overall aim of the GDPR is to improve transparency, accountability and governance. The Council will have to be clear with residents and others what data it is collecting and what is done with it. The Council will be liable for any breach of the GDPR and must make sure there are proper controls in place to protect personal data.

1.3 The GDPR requires all public authorities to appoint a Data Protection Officer. It is therefore proposed that the Head of Legal Services be appointed the Data Protection Officer to satisfy this requirement.

2. Resource Implications

2.1 There are no resource implications. The appointment will be assimilated into the Head of Legal Services' duties. The Information Governance Manager will assist with carrying out data protection work as part of her duties.

3. Options

3.1 The Executive has the options to agree, reject or change the proposal.

4. Proposals

4.1 It is proposed that the Executive agree that the Head of Legal Services be appointed the Data Protection Officer in accordance with the GDPR.

5. Supporting Information

5.1 The DPO responsibilities are defined in Article 39:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR and other data protection laws including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits;
- To be the first point of contact for supervisory authorities and for individuals whose data is processed.

5.2 The employer must ensure that:

- The DPO reports to the highest management level of the organisation
- The DPO must operate independently and is not dismissed or penalised for performing their task
- Adequate resources are provided to enable the DPO to meet their GDPR obligations.

5.3 Over the last few months preparations have been underway for the advent of the implementation of the GDPR by the Information Governance Manager. A Project Plan has been produced which has been based upon the guidance issued by the Information Commissioner. From this, an Information Asset Database has been produced which includes information about assets kept, where it is kept, ownership, retention and disposal. All staff are required to attend training sessions so that they are aware of their obligations under the GDPR. Training for members will be held in March. The Information Security Policy has also been updated ready to issue to all staff.

5.4 There is still much to do including making the appointment of the DPO. For instance, the ICO advises that a review should be carried out of the contracts register and that contractual provisions should be updated to reflect the changes in the GDPR; updating Privacy Notices/Fair processing statements. There is a greater emphasis on documentation to demonstrate mitigation of any risk and have a defence in the event of a breach.

6. Corporate Objectives And Key Priorities

6.1 PERFORMANCE: we will deliver effective and efficient services better and faster.

7. Legal Issues

7.1 The GDPR clearly places new legal obligations on the Council. The Council is preparing for this in a structured way in accordance with the guidance issued by the Information Commissioner.

8. Governance

8.1 The Council will need to comply with the requirements of the GDPR and the new Data Protection Act when it is receives Royal Assent.

9. Risk Management

9.1 Failure to comply with the GDPR can place the Council at risk of a substantial fine, including failing to notify the ICO of a breach within a 72 hour period as well as a fine for the breach itself.

9.2 The level of fines is set quite high: up to 10 million Euros or 2% of annual turnover, whichever is the greatest for level 1 fines and up to 20 million Euros or 4% of annual turnover for level 2 fines. Failure to appoint a DPO is also technically a breach.

10. Consultation

10.1 No formal consultation is required. However the Council will need to advise the public on how their data will be treated in future.

Annexes	None
Background Papers	None
Author/Contact Details	Karen Limmer, Head of Legal Services Karen.limmer@surreyheath.gov.uk
Head of Service	

Consultations, Implications and Issues Addressed

Resources	**Required**	**Consulted**
Revenue	✓	✓
Capital		
Human Resources		
Asset Management		
IT		
Other Issues	**Required**	**Consulted**
Corporate Objectives & Key Priorities	✓	✓
Policy Framework		
Legal	✓	✓
Governance		
Sustainability		
Risk Management		
Equalities Impact Assessment		
Community Safety		
Human Rights		
Consultation		
P R & Marketing	✓	✓

Review Date: 22 January 2018