Corporate Governance and Standards Committee Report

Report of Director of Resources

Author: Joyce Hamilton, Principal Corporate Services Solicitor

Tel: 01483 444053

Email: Joyce.Hamilton@guildford.gov.uk

Lead Councillor responsible: Matt Furniss

Tel: 07891 022206

Email: matt.furniss@guildford.gov.uk

Date: 21 September 2017

General Data Protection Regulation: Governance Arrangements

Executive Summary

The Data Protection Act 1998 regulates how the Council uses and stores the personal data of its customers and staff. An EU Directive, the General Data Protection Regulation (GDPR) will replace the Data Protection Act. The GDPR sets out how organisations can collect and use personal data. The GDPR comes into force on 25 May 2018. Before then, the UK will pass a new law so that the GDPR applies in the UK. The GDPR applies to organisations that provide goods or services to individuals in the EU. This includes organisations outside the EU that want to provide goods or services within the EU. The GDPR (and the new law) will continue to apply in the UK after the UK leaves the EU.

The suggested governance structure to oversee the implementation and ongoing maintenance of GDPR is set out in Appendix 1.

Recommendation to Committee

That the Committee approves the Governance structure and the Officer Project Board's approach to implementing the GDPR, as set out in Appendix 1.

Reason for Recommendation:
To comply with the requirements of the GDPR by 25 May 2018.

1. Purpose of Report

1.1 This report presents the suggested approach to the implementation of the GDPR for approval by the Committee.

2. Strategic Framework

2.1 Good Corporate Governance ensures the Council maintains high standards to protect the personal data of staff and residents, underpinning the values and mission of the Council.

3. Background

3.1 The GDPR regulates how data is processed. The GDPR definition of personal data is wider than the current definition and updated to cover changes in technology since 1998. It can include things like cookies that we automatically download when we visit websites and biometric data such as fingerprints and DNA.

3.2 The overall aim of the GDPR is to improve transparency, accountability and governance. The Council will have to be clear with residents and staff 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 is proper security and controls to protect the data that is collected.

4. Financial Implications

4.1 Non-compliance with the GDPR could have a serious financial implication for the Council.

4.2 Organisations that breach the current Data Protection Act are liable to a fine, capped at £500,000. Under GDPR, organisations are liable to a fine up to 20 million Euros or 4% of turnover, whichever is higher. If a breach involves personal data of an individual, they can also claim damages.

4.3 The appointment of our Data Protection Officer will attract a payment of £3,000, which will be met through existing budgets.

4.4 Additional support to assist us in meeting the tight deadline will be provided through independent consultancy, for which financial provision has already been made.

4.5 There may be a need to recruit additional support to services that struggle with the amount of additional tasks they need to undertake as we get nearer 25 May 2018.

5. Legal Implications

5.1 The GDPR is a large document of regulations, over 80 pages. The GDPR reinforces the established legal principle that we can only collect and use personal data if it has a legitimate reason and before collecting or processing personal data, we must make sure it has a proper reason.

5.2 The GDPR sets out when the Council can collect or process personal data. The main reasons are:

- We have the consent of the data subject (the person that the data we are collecting is about)
- Processing is necessary to carry out a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation (something we must do by law)

- Processing is necessary so we can do something in particular that is in the public interest or because we are legally allowed to in order to do something that we are responsible for
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject (this reason is not applicable to public authorities)

5.3 The GDPR requires that any consent must be freely given, informed and give a clear indication of an individual's wishes. There are also special requirements for consent from children, which will affect some of our services.

5.4 The individual's rights under the GDPR include:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object; and
- The right not be subject to automated decision making and profiling

6. Human Resource Implications

6.1 The Council has a structure of officer working groups that oversees data protection. The GDPR requires organisations to demonstrate compliance; this includes training, internal audits, data protection by design and the appointment of a Data Protection Officer (DPO).

6.2 In response to the GDPR, the Managing Director has appointed our Principal Corporate Services Solicitor, Joyce Hamilton as DPO. Service Managers will nominate Council staff to be members of the Project Board to work with the DPO and the Information Rights Officer (IRO) to implement GDPR.

6.3 The DPO is not responsible for compliance with GDPR. It is the responsibility of the Council. The DPO will monitor how the Council implements GDPR and will provide advice. The DPO will report on performance to senior management and councillors and will be the Council's link with the Information Commissioner, who oversees data protection nationally.

6.4 There will be briefings and training in the coming months for all staff, councillors and parishes affected by GDPR, that will impact on the Officer Board and other members of our services and staff.

7. Operations

7.1 A Project Board will lead on the implementation of the GDPR. The Board has agreed on its approach to the implementation (gap analysis on the 12 key steps, as outlined in Appendix 1). The Board will update this Committee at each meeting and GDPR will be a standing item on the agenda for meetings of the

Executive/Management Team Liaison Group. A monitoring schedule will be presented to enable the Committee to easily identify progress with implementation.

8. Conclusion

8.1 The GDPR marks a major change in the way we must use and store personal data from 25 May 2018. We must approach the new directive very seriously and ensure that the Council treats individual data relating to customers and staff with the utmost respect and ensure that we are not subject to the financial penalties that will occur if we do not.

8.2 Officers suggest an appropriate governance structure to support the Council, members, officers and other third parties, which is set out in Appendix 1.

9. Background Papers

Regulation (EU) 2016/679 of the European Parliament and of the Council 27 April 2016 (GDPR)
http://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

10. Appendices

Appendix 1: Governance Structure and the 12 steps for the implementation of the GDPR