

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: 18 January 2018

General Data Protection Regulation: Update

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 in 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, Data Protection Act 2018) will continue to apply in the UK after the UK leaves the EU.

Recommendation to Committee

The Committee is asked to note this report.

Reason for Recommendation:

To review the Council's progress in complying with the GDPR by 25 May 2018.

1. Purpose of Report

- 1.1 This report explains action taken to progress the implementation of the GDPR by 25 May 2018.

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. Progress since 30 November 2017

- 3.1 The Data Protection Bill began its life in The House of Lords. They are currently examining the Bill, after which it will progress to the House of Commons for further scrutiny. Once approved, the Bill (subject to any tabled amendments), will receive Royal Assent and become the Data Protection Act 2018. This Act is expected to be in force by 5 May 2018.
- 3.2 The Project Board met on 20 December 2017 and discussed training and Awareness, automated systems, procedures, data protection by design, data sharing, data cleansing, current ICT software suppliers and the Senior Leader session that took place on 30 November 2017.
- 3.3 The Council's Data Protection Officer (DPO) provided feedback to the board on recent data protection training. This training provided a general overview of the GDPR and the role of the DPO. All Surrey authorities attended this course. Guildford BC is making excellent progress, and has appropriate plans in place and is so far the only Surrey authority to have appointed a DPO.
- 3.4 Board sub groups are taking forward a wide range of action points, including developing:
- systems and processes
 - corporate guidance and procedures for data cleansing
 - a training and awareness programme; and a
 - review of data sharing (internally and with external partner organisations)
- 3.5 The data cleansing sub group is tasked with developing a way forward and common process for all services to follow to manage and delete legacy personal data, which we plan to start in February 2018. They are also reviewing information asset registers and data retention schedules for all services.
- 3.6 These sub groups are working at a high level focusing on developing corporate processes to comply with the new personal rights that will be available under the Data Protection Act 2018, namely:
- Rights in relation to automated individual decision making (including profiling)
 - Rights to Data Portability
 - Right of Erasure; and the
 - Right to Rectification
- They are also reviewing the existing right to collect and process personal data.
- 3.7 The board is considering how the Council can demonstrate data protection by design, in particular, how to incorporate this into existing and new corporate processes and new corporate/major projects. The Council can achieve Data protection by design by proactively identifying risks to personal data and applying suitable measures to reduce those risks.

- 3.8 The DPO is reviewing the impact of GDPR on the security of personal data and reporting on this to CMT.

4. Financial Implications

- 4.1 If the Council fails to comply with the GDPR, there is a risk the Council could be fined up to 4% of turnover. The Council's gross income (less internal recharges) recorded in the 2016-17 statement of accounts was £69 million, so a fine of 4% could be up to £2.76 million.
- 4.2 There are no other financial implications arising from this report.

5. Legal Implications

- 5.1 There are no other legal implications arising from this report.

6. Human Resource Implications

- 6.1 There are no human resource implications arising from this report.

7. Conclusion

- 7.1 The GDPR marks a major change in the way the Council must use and store personal data from 25 May 2018. The Council has begun work to raise awareness of the GDPR and its impact, to audit the information the Council holds, to review the Council's privacy notices and to review Council procedures. This will ensure the Council is compliant with the GDPR in how it processes the personal data of individuals.

8. Background Papers

[Corporate Governance Standards Committee Item 7 - 21 September 2017](#)
[Corporate Governance Standards Committee Item 7 – 30 November 2017](#)

9. Appendices

None