12 March 2018

Policy, Projects and Resources Committee

Preparation for General Data Protection Regulation – GDPR

Report of: *Philip Devonald – Corporate & Information Governance Lawyer*

Wards Affected: *All*

This report is: *Public*

1. Executive Summary

1.1 On 25 May 2018, the General Data Protection Regulation (GDPR) will come into full force. In addition, the Data Protection Bill 2017 will effectively adopt GDPR directly into English law. The new Act will therefore have three main themes:

- Extending the scope of data regulation
- Empowering individuals to have greater control over their own data
- Building privacy into products and services
- Imposing big sanctions for non-compliance

1.2 Members considered a report on progress at the January meeting and this report provides a further update. The Council has continued to make progress towards introducing GDPR compliant measures in time for the new law coming into effect in three months' time.

1.3 Members are asked to consider and adopt a raft of policies to ensure compliance with new data protection legislation.

2. Recommendations

2.1 **That the attached updated compliance action plan (Appendix A), be approved to enable officers to roll out effective GDPR compliance across the Council by 25 May 2018.**

2.2 **That Members note and approve the following additional revised and updated policy documents:**

- **Data Protection Policy;**
- **Data Breach Policy;**
- **Consents Policy;**
- **Data Processing Impact Assessments Policy;**
- **Privacy Notices Policy; and**
- **Clear Desk Policy,**

with delegated authority granted jointly to the Head of Legal Services and the Senior Information Risk Officer to revise and update once the details of the new Data Protection Act are known.

3. Introduction and Background

3.1 Data protection law requires individuals' personal data we hold to be processed securely, with severe and newly increased penalties for non-compliance. For this purpose, as part of the Council's general review of information governance, the Council is developing a new suite of data protection policies and procedures.

3.2 All relevant staff have been engaged to complete an online data protection training module based on these policies, during November and December 2017. This training module has now been made available to all Members.

3.3 The General Data Protection Regulation (GDPR) entered into force on 24 May 2016. However, enforcement of the GDPR will not begin until **25 May**. Organisations therefore have a limited window in which to ensure that their data processing activities are compliant with the requirements of the GDPR. The national laws implementing the Directive in each Member State will continue to apply until the GDPR Effective Date. However, the process of becoming compliant with the GDPR will take much planning and a significant amount of time. A Data Protection Bill is currently before Parliament and this will effectively adopt GDPR when enacted in due course. At the time of writing, the bill is awaiting its second reading in the House of Commons (5th March), having completed all stages in the House

of Lords. The bill is substantial, containing nearly 200 sections and 18 schedules.

3.4 The Council has therefore commenced work on its strategy for introducing GDPR compliant measures in time for the new law coming into full effect in May 2018.

4. Issue, Options and Analysis of Options

4.1 The main issue continues to be achieving effective buy-in from all staff across the Council. To this end, the Chief Executive has published on the Council's intranet a message to all staff explaining GDPR is coming and that all staff need to cooperate with actions as directed by the GDPR senior officer steering group, established to oversee the project. GDPR is a mandatory statutory requirement so the only available option is to comply with the new legislation.

4.2 The rules regarding subject access requests (SAR) will also change. Currently the Council can charge a £10 fee to respond to a SAR. Under the GDPR, no fee can be charged regardless of volume or complexity (unless the request is deemed "extreme"). The response time for responding is reduced from 40 days to one month.

4.3 The sharing of any personal data represents a potential risk under the new regime and this risk must be managed. Thus, data processing or sharing contracts must have specific terms included in them to ensure security and compliance with the data principles and existing contracts extending beyond May 2018 will need to be reviewed and possibly re-negotiated. A data sharing protocol is therefore proposed to be adopted. This will be brought before Members for consideration at a later meeting.

4.4 Another issue is that of document/data retention. In the absence of any specific legal requirements, personal data may only be retained as long as necessary for the purpose of processing. This means data must be deleted e.g. when: the data subject has withdrawn consent to processing, a contract has been performed or cannot be performed anymore, or the data is no longer up to date. Specifically we will need to develop a consistent rule for the retention of e mails; this should not be difficult as Outlook allows this to be done automatically once the rubric has been agreed. Consideration will also have to be given to the following issues:

- Has the data subject requested the erasure of data or the restriction of processing?
- Is the retention still necessary for the original purpose of processing?
- Does an exception apply to the processing for historical, statistical or research purposes?

4.5 Members are asked to consider and approve a revised and updated set of policies and procedures which it is hoped will inform the public of their rights and guide staff as to how they must handler personal data in the future. These consist of:

- An overarching Data Protection Policy (Appendix B).

- A Data Breach Policy (Appendix C). Under Article 33 of the GDPR the Council will have a new duty to report data protection breaches to the Information Commissioner and, in certain circumstances, to the individual whose personal data has been the subject of the breach. There is no legal requirement to do this under the current law. The policy/protocol has been drafted to set down the rules and procedures for staff in the event of a data breach.

- An Information Security Policy (Appendix D). Article 32 of the GDPR (Security of processing data) requires organisations to take necessary technical and organisational measures to ensure a high level of information security. The Council has already agreed a raft of measures to achieve this including policies covering access control, e mail policy, acceptable use as well as combined information security controls.

- A Consents Policy (Appendix E). This has changed significantly under the GDPR. Consent to processing personal data must be active and does not rely on silence, inactivity or pre-ticked boxes, is not bundled with other agreements supply of services is not made contingent on consent to processing which is not necessary for the service being supplied, data subjects are informed that they can withdraw consent and that there are simple methods for doing so.

- A Data Processing Impact Assessments Policy (Appendix F). Under Article 35 of the GDPR, where a type of data processing is likely to result in a high risk for the rights and freedoms of individuals, data controllers are required to carry out a DPIA prior to the processing to assess the impact of the proposed operation or change on the protection of personal data.

- A Privacy Notices Policy (Appendix G). The GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are more detailed and specific than in the DPA and place an emphasis on making privacy notices understandable and accessible. Data controllers may need to include more information in their privacy notices. The GDPR says that the information you provide to people about how you process their personal data must be concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge.

- A Clear Desk Policy (Appendix H) which is self-explanatory.

5. Reasons for Recommendation

5.1 Members have approved a compliance action plan and project plan. This is a complex, council wide project so that some dates for action/completion under the project plan are subject to change for operational reasons. In addition, the law in terms of a new Data Protection Act is not yet enacted and further changes to the detail may be possible. This will not affect the overall projected completion date of 25 May 2018, though some on-going work will be necessary.

5.2 Specific work flows will be developed following receipt of council-wide responses to a questionnaire which has been sent out to all departments, along with guidance notes and other documents. This is vital to capture all information necessary to ensure compliance in all areas in due course, both hard copy and electronic. The deadline for responses is 12th March. After that we will analyse the information and categorise it. A programme of review and deletion of outdated material will then follow. Specific GDPR training will be put in place for both officers and Members to complete over the coming months.

6. Consultation

6.1 No consultation is required in advance of submission of this report to Committee.

7. References to Corporate Plan

7.1 With regard to the priority: 'Community and Health' this report supports businesses, safeguards public safety and enhances standards locally through risk-based regulatory compliance with the Data Protection Act 1998 and the forthcoming GDPR.

8. Implications

Financial Implications
Name & Title: Jacqueline Van Mellaerts, Financial Services Manager
Tel & Email: 01277 312 829
jacqueline.vanmellaerts@brentwood.gov.uk

8.1 Risk of up to €20.0m (£17.7m) fine for non-compliance with GDPR with associated financial consequences and potential reputational harm to the Council.

8.2 Currently the additional resources required for the implementation of GDPR by May 2018, consists of an Interim Corporate & Information Governance Lawyer and is being funded from the Council's Reserves due to the transformational activity. There will also be a cost of providing training to staff and Members, which is covered by existing budgets.

Legal Implications
Name & Title: Daniel Toohey, Head of Legal Services and Monitoring Officer
Tel & Email: 01277 312 860 daniel.toohey@brentwood.gov.uk

8.3 Legal issues and implications are set out in the body of this report and appendices.

9. Background Papers (include their location and identify whether any are exempt or protected by copyright)

9.1 GDPR project plan summary.

10. Appendices to this report

- Appendix A - Updated GDPR Compliance Plan
- Appendix B - Data Protection Policy
- Appendix C - Data Breach Policy
- Appendix D - Information Security Policy
- Appendix E - Consents Policy
- Appendix F - Data Processing Impact Assessments Policy
- Appendix G - Privacy Notices Policy
- Appendix H - Clear Desk Policy

Report Author Contact Details:

Name: Philip Devonald, Corporate & Information Governance Lawyer
Telephone: 01277 312 707
E-mail: Philip.devonald@brentwood.gov.uk