EXECUTIVE - 22 MARCH 2018

GENERAL DATA PROTECTION REGULATION (GDPR)

Executive Summary

This report presents the progress made at the Council on compliance with the EU's General Data Protection Regulation (GDPR) and the work that must still be carried out. It also includes a draft of a new Data Protection Policy which will assist in compliance.

The GDPR comprises of three main parts: the principles on which personal data should be processed, the lawful bases on which organisations can rely on and the rights available to individuals. There are also provisions relating to accountability and good governance which should be adhered to.

A significant portion of the compliance work necessary has already been carried out by a GDPR Steering Group, including an audit of current personal data processing activities across the Council. This audit, along with the guidance from the Information Commissioner's Office, has allowed the Steering Group to recommend to the Corporate Management Group specific actions in order to achieve compliance. Those which can be carried out centrally have been assigned the responsibility of the Steering Group, while for those that concern the personal data processing activities of the Sections themselves, the Steering Group will work with CMG members to provide the tools and guidance necessary.

The two aspects of the report requiring a decision by Full Council are the adoption of a new Data Protection Policy and the appointment of Peter Bryant (Head of Democratic and Legal Services/Monitoring Officer) as Data Protection Officer.

Reasons for Decision

Consideration of these matters will enable the Council to comply with the EU's General Data Protection Regulation when it comes into force in May 2018.

Recommendations

The Executive is requested to:

RECOMMEND to Council That

(i) the progress made on compliance with the General Data Protection Regulation, as well as the need for further work, be noted;

(ii) the draft new Data Protection Policy be adopted; and

(iii) Peter Bryant (Head of Democratic and Legal Services/Monitoring Officer) be appointed Data Protection Officer.

This item will need to be dealt with by way of a recommendation to the Council.

Background Papers:

Sustainability Impact Assessment
Equalities Impact Assessment

Reporting Person:

Peter Bryant, Head of Democratic and Legal Services/Monitoring Officer
Ext. 3030, E Mail: Peter.Bryant@woking.gov.uk

Contact Person:

Robert Bishop, Graduate Trainee
Ext. 3001, E Mail: Robert.Bishop@woking.gov.uk

Portfolio Holder:

Cllr Ayesha Azad
E Mail: CllrAyesha.Azad@woking.gov.uk

Shadow Portfolio Holder:

Cllr Ann-Marie Barker
E Mail: CllrAnn-Marie.Barker@woking.gov.uk

Date Published:

14 March 2018

1.0 Introduction

1.1 The impact on the Council of the EU's General Data Protection Regulation (GDPR) was first considered by the Corporate Management Group (CMG) on 24 July 2017, when a high-level briefing was presented. On 16 October 2017, a timetabled Action Plan, based on the Information Commissioner's Office compliance guidance, was presented to the CMG and approved.

1.2 Since that meeting, the execution of this Action Plan has been carried out by a GDPR Steering Group, formed of Robert Bishop (Graduate Trainee and Project Manager for GDPR Compliance), Adele Devon (ICT Manager), Jacqueline Hutton (Solicitor), Pino Mastromarco (Senior Policy Officer) and Sarah Reed (Principal HR Advisor).

1.3 Definitions used in the GDPR and in this report are as follows:

- '**Personal data**' is any information relating to an identified or identifiable natural person, either through their name or another identifier such as an identification number.

- '**Processing**': any operation performed on personal data, whether or not by automated means, such as collection, use or disclosure. It should be noted that the GDPR applies to processing of personal data in hard copy form as well as by electronic means.

- '**Data subject**' is the term used to describe any given person when identified in relation to their personal data.

- '**Data controller**' is the label for organisations which decide how and why personal data is used, while '**data processors**' is a label for organisations responsible for processing personal data on behalf of a controller. Woking Borough Council is a data controller, while its suppliers are data processors.

- '**Special categories**' of personal data encompasses ethnicity and data concerning health, among other categories. To process these, there are extra requirements. Similar requirements exist in the GDPR for processing data on criminal convictions or offences.

2.0 The GDPR

2.1 The GDPR, along with the Data Protection Bill currently going through the UK Parliament, will represent the new data protection regulatory regime after 25 May 2018. The GDPR's purpose is to bring data protection law in Europe up to date, which has not changed significantly since the late 1990s. In the UK, it will replace the Data Protection Act 1998 ('DPA'). It should be noted that the GDPR represents an evolution of the current law, and the existing compliance infrastructure whose purpose is to meet the requirements of the DPA will still be relevant, necessary and useful.

2.2 The purpose of the Data Protection Bill is to 'fill in the gaps' where the GDPR provides them for EU member states. These gaps allow member states to legislate to exempt some principles in the GDPR from certain kinds of personal data processing. These exemptions will be taken into account when achieving compliance at the Council.

2.3 The GDPR lays out six principles for personal data processing (Article 5), which are very similar to those in the DPA. They dictate that personal data shall be:

5(1)(a) Processed according to the law, fairly and in a transparent manner;

5(1)(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;

5(1)(c) Adequate, relevant and limited to what is necessary in relation to the purpose;

5(1)(d) Accurate and, where necessary, kept up to date;

5(1)(e) Kept for no longer than is necessary for the purpose; and

5(1)(f) Processed in a manner that ensures appropriate security of the personal data.

As well as these principles, there is a requirement that data controllers:

5(2) "shall be responsible for, and be able to demonstrate, compliance with the principles".

2.4 In order to process any given personal data, the organisation undertaking the processing must identify a lawful basis for that processing (Article 6). There are six available lawful bases, similar to the 'grounds for processing' in the DPA. No single basis is 'better' than the others – which basis is most appropriate in each case depends on the purpose for that processing and the relationship with the data subject.

6(1)(a) The data subject has given clear **consent**

6(1)(b) The processing is necessary for a **contract** with the data subject

6(1)(c) The processing is necessary to comply with the **law**

6(1)(d) The processing is necessary to protect someone's **life**

6(1)(e) The processing is necessary for you to perform a task in the **public interest** or for an organisation's **official functions**, and the task or function has a clear basis in law.

6(1)(f) The processing is necessary for an organisation's **legitimate interests** or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

In order to process special categories of personal data, both a lawful basis must be identified from the list above, as well as an additional lawful basis from another list (Article 9). A similar mechanism is included in the GDPR concerning the processing of personal data on criminal offences or convictions (Article 10).

2.5 The aspect in which the GDPR extends furthest beyond the DPA is rights. Under the GDPR, data subjects are afforded:

- The right to be **informed**: data subjects must be told the purpose for which their personal data is being processed, any other recipients of their personal data and the existence of their rights, among other information, at the first available opportunity.

- The right of **access**: data subjects can obtain confirmation that their data is being processed, access to that personal data and other supplementary information, free of charge.

- The right to **rectification**: data subjects can have their personal data rectified if it is inaccurate or incomplete.

- The right to **erasure**: under certain circumstances, an individual may have their personal data erased. It should be noted that this does not apply to personal data processed on the lawful bases of statutory obligation and public interest or official authority.

- The right to **object**: data subjects can object to their personal data being processed, and depending on their personal circumstances and the lawful basis used, its processed may have to be restricted, at least temporarily.

- The right to **data portability**: if the personal data is processed on the lawful basis of consent or a contract, data subjects have the right to receive their personal data in such a format that is structured, commonly used and machine readable.

- In cases where personal data is used to analyse data subject's behaviour, performance or movements or to make decisions about them through **wholly-automated means**, data subjects are afforded with additional, specific rights.

2.6 Children have the same rights under the GDPR as adults, and the same principles from Article 5 apply to the processing of their personal data. However, it should be noted that, if consent is relied upon as the lawful basis when offering an online service directly to a child, only children aged 13 or over are able to provide consent. Privacy notices aimed at children should also be written in a way in which they understand.

2.7 The GDPR includes provisions that promote accountability and good governance. In order to fulfill Article 5(2) (see paragraph 2.3), the Council must:

- Implement technical and organisational measures that ensure and demonstrate compliance;

- Maintain documentation on processing activities;

- Appoint a Data Protection Officer;

- Undertake and record Data Protection Impact Assessments, where appropriate;

- Review contractual arrangements with suppliers to ensure that their use of personal data is governed by appropriate standard clauses; and

- Review procedures for detecting, investigating and reporting personal data breaches.

3.0 Compliance activity

3.1 The requirements under the GDPR detailed in Section 2 above have dictated the compliance activity taking place at the Council. As identified in paragraph 1.1, a GDPR Steering Group has been guiding compliance activity according to those requirements.

3.2 The original timetable for GDPR compliance activity, included in the report on GDPR to the Corporate Management Group meeting of 25 September 2017, is included as follows:

September 2017 – March 2018	Raise awareness of GDPR within the Council; Document personal data held by the Council; Review privacy notices; Review procedures to ensure that individuals' rights are protected (this includes amending contracts and updating software systems); Updating procedures for dealing with subject access requests; Identify the lawful basis on which personal data is processed; Review procedures for detecting, investigating and report data breaches Assess situations where it will be necessary to carry out a Data Protection Impact Assessment; Designate a Data Protection Officer.
22 March 2018	Report to Executive
26 March 2018	Report to Overview and Scrutiny Committee
5 April 2018	Report to Council
9 April 2018 – 24 May 2018	Delivery of e-training for staff

3.3 The most significant task thus far has been the detailed audit of personal data processing activities at the Council and by its wholly-owned companies. This has resulted in an Information Asset Register of over 400 individual inbound and outbound 'flows' of personal data being identified.

- In short, the detail recorded in it allows CMG members and their Sections to improve the security of their data processing operations and to make sure they are GDPR-compliant by 25 May in a targeted way.

- After this date, maintenance of the Information Asset Register will allow the Council to fulfil the requirement in Article 30 to document personal data processing activities.

3.4 The Steering Group has identified a legal basis for all of the data processing in the Information Asset Register. To the Council's advantage, large amounts of personal data processing can be justified on the basis of a statutory or contractual obligation. The remaining processing must be justified on alternative legal bases. In addition, regardless of the legal basis, a Data Protection Impact Assessment might be necessary. This is a small number of cases and those cases are identified in the Information Asset Register.

3.5 Adherence to the GDPR principles will be strengthened by:

- Provision of **e-training** to officers, separate e-training to members and a guidance document for officers and volunteers who do not use a PC. An awareness campaign will also be undertaken in the Civic Offices, including posters in the offices and notices on the staff intranet.

- Enforcement of new corporate **retention periods** for both digital and hard copy content. These are being implemented as part of migration from SharePoint 2010 to SharePoint 2016, and for hard copy, CMG members have been made aware that a proportion of the personal data residing in the Council's archives may have to be disposed of.

- Enhanced **security measures** for both digital and hard copy content. First, personal data will be protected following restriction and closure of existing shared drives and migration to SharePoint 2016. Second, where large amounts of personal data or any amount of special categories of personal data are being stored in hard copy, locks will be provided.

- Use of **new privacy notices** provided upon collection of personal data from data subjects, such as at the end of paper forms or digital e-forms.

- Implementation of **updates to ICT systems**, such that they have GDPR-compliant functionality, including the ability to erase personal data without trace and to hold information on whether consent has been offered by a data subject.

- An **update to the website** page on Data Protection and the creation of a new inbox to receive information rights requests (for those rights outlined in paragraph 2.5).

- Appointment of Peter Bryant (Head of Democratic and Legal Services/Monitoring Officer) as **Data Protection Officer** ('DPO'), a statutory position required by the Regulation. Mr Bryant is currently the Council's Senior Information Risk Owner, a role with which the responsibilities of a DPO are closely associated.

3.6 Members of the Steering Group attended the Corporate Management Group on 19 February to report on the progress of the compliance activity and to gain approval for necessary compliance actions, including those outline above. Appendix 2 of the report written for that meeting delineated responsibility for those actions.

- Many could be completed centrally by the Steering Group or the Steering Group in liaison with one other Section.

- However, others cut across many sections and depend on the personal data processing activities each carries out. For these, it was decided that the tools necessary to remedy specific compliance issues would be provided by the Steering Group to those sections through their relevant CMG members. These tools include a relevant excerpt of the Information Asset Register, a self-assessment 'process map' to direct them towards compliance, a template for a Data Protection Impact Assessment and the standard letter and clauses for varying contracts.

4.0 Wholly-owned companies

4.1 Meetings have been held with representatives of wholly-owned companies – Brookwood Park Ltd and the Thameswey Group – in order to assess their readiness for the GDPR.

- No major compliance issues were identified for Brookwood Park Ltd. Regardless, they will be included in the same compliance process as WBC Sections.

- Thameswey Group's Data Manager has already started to prepare that organisation for GDPR. The Steering Group will be in frequent contact to share material and track progress in the lead up to 25 May 2018.

5.0 Policy change

5.1 Guidance from the Information Commissioner's Office recommends that in order to meet the accountability and good governance requirements of the GDPR, organisations review and update their internal policies.

5.2 In order to prepare for the GDPR, a new Data Protection Policy has been drafted (attached as Appendix 1). This deals with the 'high level' principles of data protection. Guidance notes detailing how these principles will be complied with will be drafted subsequently and appended to the policy. These guidance notes will be approved by the Data Protection Officer.

5.3 Paragraph 5.4 of the amended Data Protection Policy deals with members registering, on an individual basis, with the Information Commissioner's Office. Where a member processes personal information on behalf of the Council (e.g. as a Committee member), he/she does so under the Council's registration. When members process personal data whilst acting as a Ward Councillor (e.g. casework on behalf of individual residents), they do so as data controllers in their own right, and should have a separate "registration" with the Information Commissioner. As part of the changes resulting from the GDPR, any "registration" requirements for members will be dealt with by the Data Protection Officer.

6.0 Implications

Financial

6.1 The annual fee payable by the Council to the Information Commissioner's Office will rise from £500 to £2,900.

6.2 It is anticipated that the fee payable to register each member with the Information Commissioner will be £35-£40. An allowance of £1,200 should be made for this activity.

6.3 No further budgetary needs have been identified in order to achieve GDPR compliance, except for those that fall within existing budgets:

- Separate GDPR e-training for staff and members.

- Updates to ICT systems, such that they have GDPR-compliant functionality.

Human Resource/Training and Development

6.4 The need for updated data protection e-training for all staff has been identified. This is currently being sought through Surrey Learning Pool, who are providing GDPR e-training to other Surrey district councils. It is expected that this e-training will be rolled out to staff between 9 April 2018 and 24 May 2018 and will form part of the mandatory training for new starters thereafter.

6.5 The LGA is in the process of producing an e-training package for members. If ready in time, this will form part of the training provided to members in the new municipal year. If the LGA training package is not ready, alternative training will be provided.

Community Safety

6.6 The Multi-Agency Information Sharing Protocol (MAISP) managed by Surrey County Council currently governs information sharing relating to Community Safety. It is constructed and operates within the confines of the DPA. Woking Borough Council will continue to take direction from Surrey County Council on any changes to the MAISP in light of GDPR.

Risk Management

6.7 The Council will be at risk of not complying with its statutory obligations if it does not take action in light of the new data protection legislation.

Sustainability

6.8 There are no specific sustainability impacts.

Equalities

6.9 There are no specific equalities impacts.

7.0 Conclusion

7.1 Progress on compliance with the GDPR is being made at good pace and the Council is on track to achieve compliance by the in-force date of 25 May 2018.

7.2 The Overview and Scrutiny Committee will be invited to comment on this report and the work at the Council surrounding GDPR compliance at its meeting on 26 March 2018. The views of the Overview and Scrutiny Committee will be reported to Council.

REPORT ENDS