AUDIT GOVERNANCE AND STANDARDS COMMITTEE	**20 November 2017**

Update on the General Data Protection Regulation

Final Decision-Maker	To be noted
Lead Head of Service	Angela Woodhouse, Head of Policy, Communications and Governance
Lead Officer and Report Author	Lead Officer: Angela Woodhouse Report Author: Anna Collier, Policy and Information Manager
Classification	Public
Wards affected	All

Executive Summary

This report provides a briefing on the General Data Protection Regulation (GDPR) that will replace the Data Protection Act (1998), coming into force on 25 May 2018. It also outlines the actions required to prepare for the changes.

This report makes the following recommendations to this Committee:

1. The update on the General Data Protection Regulation be noted.

Timetable	
Meeting	***Date***
Audit Governance and Standards Committee	20 November 2017

Update on the General Data Protection Regulation

1. INTRODUCTION AND BACKGROUND

1.1 The purpose of this report is to provide a briefing on the General Data Protection Regulation (GDPR) that will replace the Data Protection Act (DPA) (1998), coming into force on the 25 May 2018.

1.2 The report provides an overview of GDPR and additional or changed responsibilities from the current DPA compliance responsibilities.

1.3 The report outlines the action that is required to prepare for these changes.

---

2. BRIEFING ON GDPR

2.1 When the GDPR takes effect on the 25 May 2018, it will replace the Data Protection Directive (Directive 95/46/EC) which regulates the processing of personal data across the EU. In the UK, the Data Protection Act (DPA) is based on the Directive; these regulations will replace the Data Protection Act (1998). The GDPR unifies, modernises and harmonises data protection rules across all member states in the EU.

2.2 The Government has confirmed that it will implement the GDPR, but also has the ability to apply 'flexibility' in over 50 of the provisions contained in the Articles. There is still uncertainty as to new data protection legislation in the UK (including the application of the 'flexibilities'), and the Information Commissioner's Office (ICO) has not yet completed final guidance on a number of topics. But implementation of the GDPR does not require any UK legislation.

2.3 Discretionary fines can be imposed along with other measures. There are two tiers of fines - €10m-€20m, equivalent to £9m - £18m, or 2%-4% of global turnover (whichever is higher). Individual governments can decide whether public authorities should be subject to fines and if so the amounts (possibly similar to existing monetary penalties).

Changes under GDPR

2.4 Principles are reduced from eight to six (outlined below). They are similar to those in the DPA and include a new 'Accountability' requirement:

- Lawfulness, Fairness and transparency
- Purpose Limitation
- Data Minimisation
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

2.5 The GDPR makes many changes to EU data protection law but it is not a complete departure from existing principles and many of the concepts will be familiar from current DPA requirements. The most significant addition is the requirement under GDPR for organisations to show how they comply with the principles – for example by documenting the decisions taken about a processing activity. The Council has undertaken a lot of work in the past few years on data protection and information management, which provides a good foundation to build from. The differences between the current Data Protection requirements and GDPR are set out at Appendix A as a high level summary table. There are new elements and significant enhancements which the Council will need to plan for to ensure compliance with the regulations.

2.6 When collecting personal data we currently have to give people certain information, such as our identity and how we intend to use their information. This is usually done through a privacy notice. GDPR enhances this process. For example, an explanation is required of the lawful basis for processing the data, data retention periods must be specified and individuals have a right to complain to the ICO if they think there is a problem with how their data has been handled. GDPR also requires the information to be provided in concise, easy to understand and clear language.

2.7 The rights individuals will enjoy under the GDPR are the same as under the DPA but have been enhanced and strengthened. The GDPR includes the following rights for individuals:

- 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 to be subject to automated decision-making including profiling.

2.8 Highlighted below are key areas of change that will affect the council following GDPR.

<u>Processing Data</u>

2.9 Under GDPR the organisation will have to understand the lawful basis for processing personal data. The lawful basis for processing data must be documented in the privacy notice. In reality, a majority of the Council's processing activities are lawful but consideration will need to be given whether all personal data collected and processed is lawful.

2.10 Rules on consent to process information have been updated. Consent must be freely given, specific, informed and unambiguous and require a positive opt in. The Council must also consider whether consent is appropriate and an alternative would be more appropriate.

2.11 GDPR has brought in special protection for children's personal data. Online services to children that rely on consent to collect information about them may need a parent or guardian's consent in order to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16. If a child is younger then we will need to get consent from a person holding 'parental responsibility'.

The right to erasure or the right to be forgotten

2.12 Individuals will have the right to have their data deleted if there is no lawful basis for processing their data and/or in situations when consent for processing is required.

2.13 The right is not absolute and can be refused in specific circumstances. For the Council a majority of information is collected in GDPR terms

'to comply with a legal obligation or for the performance of a public interest task or exercise of official authority'.

2.14 It is therefore essential that all services review whether all personal information collected in a process can be proved to be for that purpose.

The right to rectification

2.15 Individuals are entitled to have personal data rectified if it is incorrect. The Council must respond within one month (though this can be extended to two months if complex). If the information has been shared with a third party then this must also be declared.

Subject Access Requests

2.16 Subject Access Requests aren't new but there have been changes to the rules:

- We cannot charge for complying with a request (in a majority of cases).
- We have a month to comply, rather than the current 40 days.
- We can refuse or charge for requests that are manifestly unfounded or excessive.
- If we refuse a request, we must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. We must do this without undue delay and at the latest, within one month.

2.17 Maidstone does not apply the charge so there will no impact from the charge being removed.

Data Breaches

2.18 The Council already has a responsive approach to investigating reports of data breaches. Currently it is best practice to report any breach to the ICO. GDPR makes reporting mandatory if there is a risk to the individual's rights and freedoms.

2.19 The breach should be reported in no less than 72 hours of becoming aware of it and the ICO will have the ability to issue fines for failing to notify and failing to notify in time.

Privacy by Design

2.20 The GDPR makes privacy by design mandatory. It also makes Privacy Impact Assessments, referred to as 'Data Protection Impact Assessments' or DPIAs mandatory in certain circumstances.

2.21 A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals;
- where there is processing on a large scale of the special categories of data;
- if a DPIA indicates that the data processing is high risk, and we cannot sufficiently address those risks, we will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

3. Data Protection Officer

3.1 The GDPR includes provisions that promote accountability and governance. Article 24(1) places an explicit legal obligation on controllers, and for the first time processors, to ensure and be able to demonstrate that all processing is undertaken in compliance with the requirements of the GDPR. This includes for example collecting records of processing operations for organisations with 250 or more employees and ensuring data privacy impact assessments (DPIAs) are undertaken when required.

3.2 The Council is now required to create or designate an officer to be responsible for data protection and ensure compliance. GDPR sets a number of rules around this role which ensure that the Data Protection Officer (DPO) has the knowledge, support and authority to carry out their role. Details of the role are set out in Appendix B.

3.3 Although Data Protection Officers (DPOs) are not personally liable in cases of non-compliance with the GDPR and it is the organisation that is ultimately accountable and responsible, the designation of a DPO is one of several accountability measures designed to strengthen corporate self-regulation.

3.4 Where the controller or the processor is a public authority or body, a single DPO may be employed directly by a single authority or as an agent under a service contract designated as the DPO for several authorities or bodies. Precise credentials or qualifications that DPOs must have are not specified, but it does require that the:

- DPO is designated:

    - on the basis of professional qualities, and in particular, expert knowledge of data protection law and practices with the ability to fulfil the tasks specified in Article 39
- Contact details of the DPO:
    - are published (so they are directly accessible to the public)
    - communicated to the regulator (as the primary contact person).

3.5 Further details of the role and tasks of the DPO can be seen at Appendix B.

3.6 Given existing responsibilities in the investigation of data breaches, management of subject access requests and being the named responsible officer for stage 2 complaints, the Head of Policy, Communications and Governance is now also the Council's Data Protection Officer. Additional training has been undertaken to ensure that the post holder is at GDPR practitioner level.

3.7 Additional support will be provided by the Policy and Information Manager and the Information and Corporate Policy Officer who are already responsible for supporting Data Protection.

4. PREPARING FOR THE GENERAL DATA PROTECTION REGULATION

4.1 The Information Commissioners Office has identified twelve steps that Councils should take to prepare for GDPR which align with the changes. The twelve steps are:

i. Awareness – raising awareness in the organisation
ii. Information we hold – reviewing what personal data we hold and with whom it's shared
iii. Communicating privacy information – review privacy notices
iv. Individual's rights – check our procedures to review individuals' rights including how personal data will be deleted
v. Subject access requests – update processes
vi. Lawful basis for processing data – identify the lawful basis for processing.
vii. Consent – review consents and consider whether new consents are needed.
viii. Children – Consider whether new processes are needed to verify ages or gain consent
ix. Data breaches – review and update procedures
x. Data Protection by Design and Data Impact Assessments
xi. Data Protection Officers - appoint if needed
xii. International – identify any data that is subject to international transfer

4.2 The action plan at Appendix C sets out the actions the Council needs to take, in order to prepare. It is organised under the above headings.

4.3 The key action that is being undertaken is a programme of information lifecycle audits. A copy of the form can be seen at Appendix D. These audits are helping the Council prepare under points 2, 3, 4, 6, 7, 8, 10 and 12 shown above. These forms and the related action plan which will

support delivery of any recommendations will help evidence our decision making, as GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability.

4.4 The Policy and Information Team is already working closely with Tunbridge Wells Borough Council in order to share resource and knowledge. Part of this work will be sharing training sessions, guidance and policies to reduce workload. In addition a shared resource has been identified to help implement the requirements as there are elements of the same work required at both councils. This will make the most out of the resource and encourage shared learning and practice.

4.5 Initial basic training has already taken by members of the Policy and Information team. The Head of Policy, Communications and Governance has undertaken GDPR practitioner training and further practitioner training has commenced for the Policy and Information Manager who would deputise in the Head of Service's absence. General GDPR awareness training was arranged for the Information and Corporate Policy Officer who will be supporting the Head of Service in delivery of day to day work.

---

5. RISK

5.1 Information management has already been identified as a corporate risk for the council. The action plan at Appendix C sets out steps to mitigate risk.

---

6. NEXT STEPS: COMMUNICATION AND IMPLEMENTATION OF THE DECISION

6.1 An action plan is set out at Appendix C.

---

7. CROSS-CUTTING ISSUES AND IMPLICATIONS

Issue	Implications	Sign-off
Impact on Corporate Priorities	The introduction of the General Data Protection Regulation will affect both Council priorities as it will impact on the management of all information collected, used and stored for all Council	Head of Policy, Communications and Governance

	activities unless legislation states otherwise	
Risk Management	Not preparing or sufficiently preparing for the changes introduced under GDPR leaves the Council open to significant risk. Should the Council not prepare for GDPR and the ICO investigates, the Council could be at risk of a fine.	Head of Policy, Communications and Governance
Financial	Employing additional support to help audit and implement changes will result in a financial cost to the Council. One-off budgetary provision will be made to meet this cost.	Head of Policy, Communications and Governance
Staffing	Introducing changes under GDPR will result in significant impact to officers' time. There is a substantial impact within the Policy and Information Team, possibly the ICT team and on the digital team. There will also be impact on all service managers as all process will need to be audited and recommendations implemented All staff will need to be trained and briefed on the implications of GDPR and their role in compliance.	Head of Policy, Communications and Governance
Legal	The Council has a number of legal obligations under GDPR and these have been outlined in the report. MKLS will be working with officers to amend existing contracts affected by GDPR, as well as making the necessary amendments to contract templates to be used by the Council for future agreements to incorporate the changes brought in by GDPR.	Team Leader (Contracts and Commissioning) MKLS

Privacy and Data Protection	The Council has a number of legal obligations under GDPR and these have been outlined in the report	Head of Policy, Communications and Governance
Equalities	Whilst auditing services there may be a need to change processes, EQIA may need to be completed at that time. Equalities data is personal data and can be sensitive personal data, audits will need to consider whether this data is required, alongside consideration as to whether collected the data will ensure that services are delivered equably.	Head of Policy, Communications and Governance
Crime and Disorder	Services operating within this area will be audited alongside other services	Head of Policy, Communications and Governance
Procurement	Services operating within this area will be audited alongside other services	Head of Policy, Communications and Governance

8. REPORT APPENDICES

The following documents are to be published with this report and form part of the report:

- Appendix A – GDPR comparison with Data Protection Overview
- Appendix B: Data Protection Officer Role
- Appendix C: Action Plan and Timetable for GDPR
- Appendix D: Data Process Form

---

9. BACKGROUND PAPERS

None