Classification: Private
Key Decision: No

Gravesham Borough Council

Report to:	Performance & Administration Committee
Date:	19 February 2019
Reporting officer:	Gayle Jones, Information Governance Manager & Data Protection Officer
Subject:	General Data Protection Regulations

Purpose and summary of report:

To provide Members with an overview to the introduction of the General Data Protection Regulations (GDPR) and the Data Protection Act 2018, its impact on the council and the work undertaken by the authority to ensure appropriate compliance.

Recommendations:

1. Members are asked to review the report and project plan developed with regards to the implementation of the General Data Protection Regulations and provide comments as necessary.

1. Introduction

1.1 In January 2012 the European Commission published a draft General Data Protection Regulation; following several years of negotiation and amendment, the final document was officially adopted by the European Parliament and the Council of the European Union, on 14 April 2016. The Regulation replaces Directive 95/46/EC, which was enacted in 1995, and significantly changes EU data protection laws. Following publication in May 2016, the GDPR became enforceable in UK law from May 2018.

1.2 Section 3 of the European Union (Withdrawal) Act 2018 confirms that all “direct EU legislation” that is operative before the UK’s exit will remain part of domestic law on and after that date. With the GDPR enforceable since May 2018, the UK’s departure from the European Union does not therefore impact on the continued requirement for relevant compliance.

2. GDPR overview

2.1 What is GDPR?

The GDPR is Europe's new framework for data protection laws. It replaces the previous 1995 data protection directive, upon which UK law was previously based.

The EU's GDPR website outlines that the legislation is designed to "harmonise" data privacy laws across Europe, as well as giving greater protection and rights to individuals. Within the GDPR there are large changes for the public as well as businesses and bodies that handle personal information.

2.2 The Information Commissioner's Office (ICO) is responsible for ensuring compliance with the GDPR requirements, in the same way as with the Data Protection Act. Accordingly, the Information Commissioner has been given legislative powers to take action against any organisation that fails to follow the requirements of the GDPR, or misuses personal information held by that organisation.

3. Gravesham Borough Council's response

3.1 In January 2017, Management Team was provided with a report to set out the initial 12 step program that the ICO considers should be undertaken to address the changes imposed under the GDPR.

3.2 At this time, Management Team agreed a number of actions as detailed below:

- Where GBC has not previously designated responsibility and a budget for data protection compliance it is recognised that these requirements will impose an increased financial burden – accordingly, under the shared service arrangement with Medway Council, a dedicated budget was put in place to provide the necessary resources and training activities
- The Information Governance Group (IGG), consisting of the Director (Corporate Services), Director (Environment & Operations), Head of Legal Services, Information Governance Manager, Head of Internal Audit & Counter Fraud, and several departmental representatives would formulate an action plan and oversee the project.
- Set-up working groups within each directorate to implement the action plan.
- Deliver updated Data Protection training to all staff that handle personal data in early 2018.

3.3 A detailed assessment of the risks associated with the GDPR project was subsequently undertaken with a number of officers across the council.

3.4 All risks were assessed following the council's internal approach to risk management and were scored accordingly. Suggested actions to mitigate the risks were identified and built into the overall project plan for the implementation of GDPR.

Table one below explains the ICO '12 Step Program' in more detail and the actions undertaken by GBC to deliver appropriate compliance.

Table one: GBC compliance with GDPR

Step	Description
1	**Awareness:** *Make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. Implementing the GDPR could have significant resource implications, they need to appreciate the impact this is likely to have.*
	GBC Status: The council's Management Team was made aware of the GDPR and implementation date with a report presented in January 2017. Information sessions were subsequently held for senior managers at each directorate DMT, accompanied by relevant training provided to staff and Members in January 2017 and early 2018
2	**Information you hold:** *Document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.*
	GBC Status: Forming a key part of the overall project plan, the council has a three phase plan in place for identifying improvements that are needed to comply with the data processing and accountability element of GDPR: • Phase one – record retention schedule • Phase two – information asset register • Phase three – information audit Sub-groups within each of the Council's Directorates are currently working their way through all stages of the project plan to implement the required changes.
3	**Communicating Privacy Information:** *Review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.*
	GBC Status: This forms part of the overall project plan that is being progressed through the Directorate sub-groups. Changes that have been made already include updating on the privacy notices on various forms, letters and pieces of correspondence produced by the Council's services and an update to the data processing information and Privacy Notices on the Council's website.
4	**Individuals' Rights:** Check procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
	GBC Status: This forms part of the overall project plan that is being progressed through the Directorate sub-groups. Changes that have been made already include updating on the privacy notices on various forms, letters and pieces of correspondence produced by the Council's services and an update to the data processing information and Privacy Notices on the Council's website. Individuals rights are reviewed in Data Protection Impact Assessments, see further information below at step 10.
5	**Subject Access Requests:** *Update procedures and plan how you will handle requests within the new timescales and provide any additional information.*
	GBC Status: Subject access request procedures have been reviewed, and further information is distributed to departments at the point at which a Subject Access Request (SAR) is received. This process is now managed centrally through the shared Information Governance Team, providing additional support to staff handling the requests and the individual making the request.
6	**Legal Basis for Processing Personal Data:** Look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.
	GBC Status: This forms part of the overall project plan that is being progressed through the Directorate sub-groups. Changes that have been made already include updating on

	the privacy notices on various forms, letters and pieces of correspondence produced by the Council's services and an update to the data processing information and Privacy Notices on the Council's website. The 'Three Phase Plan' has been drafted to account for these processing requirements. The basis for processing is reviewed in Data Protection Impact Assessments, see further information below at step 10.
7	**Consent:** *Review how you are seeking, obtaining and recording consent and whether you need to make any changes.*
	GBC Status: Where necessary, consent is now sought for the obtaining and recording of personal data, and practical examples of this are in relation to sign-up procedures for the Council's electronic version of Your Borough, where all recipients have had to provide their explicit permission for the Council to hold their personal data and use it to communicate with them on a regular basis.
8	**Children:** *Think now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.*
	GBC Status: This forms part of the overall project plan that is being progressed through the Directorate sub-groups. Changes that have been made already include updating on the privacy notices on various forms, letters and pieces of correspondence produced by the Council's services and an update to the data processing information and Privacy Notice on the Council's website. Changes have been made to the Council's Safeguarding polices to take about of this requirements. The processing of children's data is reviewed in Data Protection Impact Assessments, see further information below at step 10.
9	**Data Breaches:** *Make sure you have the right procedures in place to detect, report and investigate a personal data breach.*
	GBC Status: The Information Governance Group now has specific responsibility for the consideration and reporting of any personal data breach identified within the authority, and training has been provided to front-line data handlers to enable them to identify instances where data could have been breached. Such instances are rare, and tend to relate solely to human error or printing issues, with no requirement to report any data breaches to the ICO at this time.
10	**Data Protection by Design and Data Protection Impact Assessments:** *Familiarise yourself now with the guidance the ICO has produced on Data Protection Impact Assessments and work out how and when to implement them in your organisation.*
	GBC Status: The GDPR makes privacy by design a legal requirement, under the term 'data protection by design and default'. It also makes Data Protection Impact Assessments (DPIA) mandatory in situations where processing is likely to result in high risk to the rights and freedoms of individuals and accordingly all new/revised system requests (involving the processing of personal data) now require a DPIA to be carried out. As such, DPIA is a formal consideration for all decision making reports as required e.g. the recently launched Corporate Plan 2019-23 Consultation requires the processing of personal information relating to resident respondents and therefore a DPIA was undertaken to support this process.
11	**Data Protection Officers:** Designate a Data Protection Officer to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.
	GBC Status: As defined by Article 39 of the Regulation, the Information Governance Manager, employed by Medway Council as part of the Legal Shared Service, has been nominated by Gravesham Borough Council as the Data Protection Officer (DPO).

12	**International:** *If your organisation operates internationally, you should determine which data protection supervisory authority you come under.*
	GBC Status: This is considered when investigating the use of cloud storage for any elements of the Council's business, with a recent example being the investigation of the cloud-based storage credentials of continuing to use Survey Monkey, with the outcome being that this was considered viable for the Council.

3.5 As can be seen work has either been completed or is significantly underway in all relevant areas, with several of them now wholly complete, and the purpose of this report is to provide Members with an update on the work that has been completed to date and to set-out a project approach for future work associated with GDPR compliance.

4. Project Management

4.1 The project is monitored by the Information Governance Manager and the Information Governance Group as a whole to ensure that the council meets its objectives in terms of GDPR implementation.

4.2 It is intended to bring regular updates to Management Team and Members to provide a comprehensive overview of the progress the council is making towards GDPR compliance. Additional reports may be brought as and when it is deemed necessary.

5. The Information Commissioner

5.1 **Elizabeth Denham** was appointed Information Commissioner in July 2016. Her key goal is to increase the UK public's trust and confidence in what happens to their personal data.

5.2 In her GDPR myth busting blog of 22 December 2017 the commissioner wrote:

'Myth #9: GDPR compliance is focused on a fixed point in time – it's like the Y2K Millennium Bug. In 1999 there was fear that New Year's Eve would see computers crash, planes to fall out of the sky and nuclear war accidentally start.

Fact: GDPR compliance will be an ongoing journey. Unlike planning for the Y2K deadline, GDPR preparation doesn't end on 25 May 2018 – it requires ongoing effort.

It's an evolutionary process for organisations – 25 May (2018) is the date the legislation takes effect but no business stands still. You will be expected to continue to identify and address emerging privacy and security risks in the weeks, months and years beyond May 2018…

Yes budgets can be tight, technology is moving fast and there's a race to keep up with competitors. But if you can demonstrate that you have the appropriate systems and thinking in place you will find the ICO to be a proactive and pragmatic regulator aware of business needs and the real world.'

5.3 The full article can be read here. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/12/blog-gdpr-is-not-y2k/

6. BACKGROUND PAPERS

6.1 Anyone wishing to inspect background papers should, in the first place, be directed to Committee & Electoral Services who will make the necessary arrangements.

IMPLICATIONS	**APPENDIX 1**
Legal	The EU General Data Protection Regulations (Reg (EU) 2016/679) (GDPR) was enacted on 25 May 2016 and as an EU Regulation the GDPR has direct effect in the UK (as an EU member state) without the need for further implementing legislation. The deadline for GDPR compliance is 25 May 2018. Organisations that fail to comply with the GDPR requirements after 25 May 2018 may be subject to significant fines (EUR10million or up to 2% of global turnover (whichever is higher) Liability in relation to matters affecting the rights of data subjects could be subject to fines of up to EUR20million or 4% of global turnover.
Finance and Value for Money	**There are no direct financial implications, however, failure to comply could result in fines from the ICO.** **Where there are any additional costs, these will be reported to MT separately.**
Risk Assessment	**See Appendix 2**
Equality Impact Assessment	**Screening for Equality Impacts**
	Question
	a. Does the decision being made or recommended through this paper have potential to cause adverse impact or discriminate against different groups in the community? If yes, please explain answer. **No**
	b. Does the decision being made or recommended through this paper make a positive contribution to promoting equality? If yes, please explain answer. **No**
	In submitting this report, the Chief Officer doing so is confirming that they have given due regard to the equality impacts of the decision being considered, as noted in the table above
Corporate Plan	Compliance with GDPR contributes to Corporate objective 4: A sound and self-sufficient council.
Crime and Disorder	Since 25 May 2018 all agencies must be able to demonstrate that they are compliant with the General Data Protection Regulations (GDPR) and accompanying Data Protection Act 2018. For the purposes of addressing crime and disorder, in working with local partner agencies the council operates within the seven key principles of GDPR concerning the processing of personal data.
Digital and website implications	There will be a need to update information provided by the council on the website
Safeguarding children and vulnerable adults	Since 25 May 2018 all agencies must be able to demonstrate that they are compliant with the General Data Protection Regulations (GDPR) and accompanying Data Protection Act 2018. For the purposes of safeguarding activities, in working with local partner agencies the council operates within the seven key principles of GDPR concerning the processing of personal data.