28 November 2018

Regulatory & Governance Committee

General Data Protection Regulation (GDPR)

Report of: *Lee Henley - Data Protection Officer*

Wards Affected: *All wards*

This report is: *Public*

1. Executive Summary

1.1 The council are making good progress in improving and embedding its processes in relation to the GDPR. This report sets out work undertaken and details further work to embed compliance throughout the council.

2. Recommendation

2.1 That the Committee note the actions being taken by the Council in relation to the GDPR.

3. Introduction and Background

3.1 The General Data Protection Regulation (GDPR) came into effect on 25 May 2018.

3.2 GDPR is a European Regulation which brings together a single piece of Data Protection Law across all EU member states. As a result of the Brexit decision, the UK Government has implemented a new Data Protection Act (Data Protection Act 2018) that will closely align with the GDPR.

3.3 GDPR introduces a higher level of accountability and evidence based compliance. Therefore, by establishing and/or adjusting governance arrangements to comply with the GDPR, the council will be confident not only that it is complying with legislation and respecting data subjects' rights, but also that it is mitigating risk appropriately and has a defence in the event of a breach.

3.4 Under the GDPR, the fines available have been significantly increased (up to 18 million euros) and may be imposed for ***any*** infringement of the Regulation, not just data security breaches.

3.5 The Information Management Team at Thurrock Council has been commissioned to provide support to Brentwood in relation to Data Protection. Thurrock commenced work at Brentwood in June 2018 and begun by carrying out a review of the existing processes.

4. Progress to date regarding GDPR

4.1 This paper captures the actions taken to ensure that the Council maintains compliance with the GDPR**.** A summary of key changes due to the GDPR, along with the estimated timeline for the completion of the work programme is detailed within the table below. **Note** – The delivery of these timeframes will be dependent on the work of the Information Asset Owners.

4.2 Organisations will always have on-going work to achieve compliance with Data Protection Legislation and work programmes will be fluid due to this. The Information Commissioner's Office has recognised this and will want an assurance that action plans are in place to move Data Protection best practice forward.

4.3 Key priorities at this stage for the Council are Training which should be rolled out during November and Records of Processing Activity work which will be a continuous on-going cycle of work.

Key Changes due to GDPR	Progress Made	Completion Timelines (Q3/Q4)
Authorities are now required to demonstrate that they comply with the new law (evidence based).	**Completed work:** • There is an existing Data Protection Policy and a range of other polices have been put in place (e.g. Retention and Data Breach Policies). • Mandatory Information Governance training has been amended to reflect GDPR changes • Individuals Rights content has been provided on the internet (public view). • Information for staff has been provided on the intranet (staff	

Key Changes due to GDPR	Progress Made	Completion Timelines (Q3/Q4)
	view). • An Information Risk Framework has been produced to identify risks to key information assets. • Contracts have been reviewed to ensure they are GDPR compliant. **Work to be completed:** • There are ongoing plans to engage with suppliers regarding the 'right to be forgotten' requirement and data portability requirement • The Information Asset Owners are currently reviewing the Document Retention Policy. • The IG training is being piloted with the aim of this being rolled out to staff in November • Information Asset Owners to undertake actions in-line with the Information Risk Framework. • To finalise the review of additional Information Governance related policies	**Q4** **Q3** **Q4** **Q4** **Q4**
Legal requirement for breach notification within 72 hours to the Information Commissioner's Officer (ICO).	**Completed work;** • A GDPR incident reporting procedure has been produced. **Work to be completed** • Update/refresh incident reporting and risk assessment form. **Note** – There have been no incidents requiring escalation to the ICO. Where incidents were reported, investigations were undertaken with appropriate feedback provided to those reporting incidents.	**Q3**
Significantly increased penalties possible for any breach of the Regulation – not just data breaches.	**Completed work:** • A comprehensive GDPR action plan has been put in place. • An Information Governance Group has been set up to drive forward the work required on	

Key Changes due to GDPR	Progress Made	Completion Timelines (Q3/Q4)
	GDPR. **Work to be completed:** • New starters to complete Information Governance training before joining the council. • A Data Protection Compliance Programme will need to be produced (e.g. Data Protection Audits).	**Q4** **Q4**
Removal of charges for providing responses to Subject Access Requests (SARs).	**Completed Work:** • A revised SAR procedure has been produced to reflect new timescales and the fact that most requests will be free of charge. **Note -** Between June and September 2018, the council received 3 SARs. All were processed within the statutory/legal timeframe.	
Requirement to keep records of data processing activities.	**Completed work:** • Information Asset Owners (IAOs) for all key areas have been identified. • On-going development of a Record of Processing Activities (RoPA) for key services. **Work to be completed:** This is a key area of GDPR. Work is on-going by the Information Governance Group to further develop their RoPA. This is key to determine: • What personal data is held, where it originated from and who it is shared with. • Do we have a legal basis for processing and is there evidence of this or are we relying on consent. • Is any data stored outside the UK. • Are fair processing notices in-line	**Q4**

Key Changes due to GDPR	Progress Made	Completion Timelines (Q3/Q4)
	with new requirements. • How consent is obtained and recorded and whether the council need to make any changes. For example, do we have evidence of consent and was it a positive form of consent (and not pre-ticked opt-in boxes). **Note**- The rules around consent only apply where the council are relying on consent as its legal basis for processing personal data.	
Appointment of a Data Protection Officer (DPO).	**Completed work:** • A DPO has been appointed.	
Data Protection Impact Assessments (DPIA) are required for high risk processing and/or when using new technologies.	**Completed work:** • A DPIA document has been produced. • The DPIA has been shared with the project team which considers new systems for the council. • The DPIA now forms part of the procurement process.	
Specific requirements for transparency and fair processing.	**Completed work:** • A GDPR compliant privacy notice has been produced. • A detailed guide on Information rights under GDPR has been produced. • An incident reporting procedure has been produced which will result in certain breaches reported to regulatory bodies. **Work to be completed:** • Mid-tier service area privacy notices to be completed and published.	**Q3**

4.4 At the Regulatory and Governance Committee on 11 July 2018 members approved the amended Regulation of Investigatory Powers Act (RIPA) policy. It was further resolved that Appendix 4 of that policy be brought to Members with this report so that, both documents could be viewed at the same time. A copy of Appendix 4 of the RIPA policy is attached (Appendix A). This contains a brief

restatement of the principles of the Data Protection Act 2018; paragraphs (a) – (f) are a word for word restatement of the recitals of Act 5 GDPR, which sets out the principles relating to the processing of personal data.

5 Implications

Financial Implications
Name & Title: Jacqueline Van Mellaerts, Interim Chief Financial Officer/Section 151 Officer
Tel & Email: 01277 312829/jacqueline.vanmellaerts@brentwood.gov.uk

5.1 There are no direct financial implications arising from this report. Costs of implementing the Data Protection Act 2018 requirements are being sought through existing resources of the Medium Term Financial Plan.

Legal Implications
Name & Title: Daniel Toohey, Monitoring Officer and Head of Legal Services
Tel & Email: 01277 312860 /daniel.toohey@brentwood.gov.uk

5.2 Legal implications are contained in the body of this report

6 Background Papers

6.1 None

7 Appendices to this report

Appendix A - RIPA policy (Appendix 4)

Report Author Contact Details:

Name: Lee Henley- Data Protection Officer
E-mail: lhenley@thurrock.gov.uk