TONBRIDGE & MALLING BOROUGH COUNCIL

GENERAL PURPOSES COMMITTEE

20 November 2017

Report of the Director of Central Services & Monitoring Officer

Part 1 - Public

Delegated

1 GENERAL DATA PROTECTION REGULATION – IMPLICATIONS FOR TONBRIDGE & MALLING BOROUGH COUNCIL

Summary
This report updates Members on the General Data Protection Regulation, highlighting the changes in data protection law that it brings about and sets out the actions being taken to ensure future compliance

1.1 Introduction

1.1.1 It has been nearly 20 years now since standards were set in the UK for data protection by the Data Protection Act 1998. Since then there has been a revolution in data and how it shapes our lives. The General Data Protection Regulation ('GDPR'), coming from the EU, is intended to address that revolution and will officially come into force on 25th May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

1.1.2 According to the European Commission the aim of the GDPR is "…to reinforce data protection rights of individuals, facilitate the free flow of personal data in the digital single market including through reduction of administrative burden."

1.1.3 The GDPR will apply to Tonbridge & Malling Borough Council and other public authorities. Our "Supervisory Authority" will remain the Information Commissioner's Office (ICO). For breaches of the GDPR the ICO will have the power to audit, issue warnings, impose temporary or permanent bans and in the case of more serious data breaches impose a fine up to 4% of a company's annual turnover or 20 million Euros whichever is the greater.

1.1.4 The core rules of data protection will remain broadly the same. However, there are new obligations under the GDPR and the requirements of the new regime will be stricter. It will be not only important to comply with the GDPR but we will also have to be able to demonstrate clearly how we comply.

1.2 Key changes

1.2.1 The use of “personal data” must comply with six data protection principles which are as follows –

(1) Data collection must be fair, for a legal purpose and be open and transparent about how the data will be used;

(2) It can only be collected for a specific purpose;

(3) The data collected must be necessary and not excessive for its purpose;

(4) It must be accurate and kept up to date;

(5) Data should not be stored any longer than necessary: and

(6) Data must be kept safe and secure.

1.2.2 Sensitive data will include genetic and biometric information.

1.2.3 Conducting criminal record checks on employees must be justified by law.

1.2.4 The GDPR sets out stricter and more detailed conditions for the use of consent. Under the new rules consent must be freely given, specific, informed and unambiguous. The onus will be on the Council to show that the data subject gave consent and if given by means of a written declaration, the request must be made in a manner that is clearly distinguishable from other aspects of the document. In addition, a data subject will have the right to withdraw their consent at any time.

1.2.5 A new right of “erasure” or “right to be forgotten” will allow someone to request that their online data is removed.

1.2.6 A new “right of data portability” will allow someone to request that their data is sent from one provider to another.

1.2.7 People must give their explicit consent for their data to be transferred outside the European Economic Area.

1.2.8 Larger companies and public authorities will be required to appoint a Data Protection Officer (DPO). The GDPR does not specify the precise credentials a data protection officer is expected to have, but it does require that this person be appointed on the basis of professional qualities and, in particular, knowledge of data protection law and practices, and the ability to fulfil the tasks set out in the Regulation i.e

To inform and advise the data controller (i.e. the Borough Council) and employees processing personal data of their obligations under the GDPR;

- To monitor compliance with the GDPR;

- To provide advice and monitor performance;
- To co-operate with the ICO; and
- To act as the contact point for the ICO on issues related to the processing of personal data.

1.2.9 The GDPR also requires that

- The DPO reports to the highest management level of the organisation;
- The DPO operates independently and is not dismissed or penalised for performing their task; and
- Adequate resources are provided to enable DPOs to meet their GDPR obligations

1.2.10 The DPO may be a staff member, or a contractor. Public bodies may have a single DPO for several such authorities, taking account of their organisational structure and size.

1.2.11 High risk data projects will require a privacy impact assessment and consultation with the supervisory authority.

1.3 Preparing for the GDPR

1.3.1 Many of the GDPR's main concepts and principles are much the same as those in the Data Protection Act 1998 so provided we are complying with the DPA then our approach to data compliance should remain valid under the GDPR. However, there are new elements and enhancements under the new regime so we will need to ensure our approach to GDPR is compliant in advance of May 2018.

1.3.2 In order to prepare for the GDPR the ICO has highlighted 12 steps that the Council can take now to prepare itself. These are as follows

(1) ***Awareness*** – Ensure that the key people at TMBC are aware of the changes being brought about by the GDPR and the impact this is likely to have (staff will need adequate and up to date training on data protection and GDPR changes);

(2) ***Information held by TMBC*** – We should document what personal data we hold, where it came from and with whom we share it. We should review the contracts and other arrangements we have in place when sharing data with other organisations. We may need to organise an information audit;

(3) ***Communicating Privacy Information*** – We should review our current privacy notices and put a plan in place for making any changes in time for GDPR implementation;

(4) ***Individuals' rights*** – We should check our procedures to ensure they cover all the rights individuals have, including how we would delete personal data or provide data electronically and in a commonly used format;

(5) ***Subject access requests*** – we should update our procedures and plan how we will handle requests within the new timescales and provide any additional information (we currently have 40 days to process a subject access request. Under the GDPR we will have to process the request within a month. We will no longer be able to charge £10 for the request);

(6) ***Legal basis for processing personal data*** – we should look at the various types of data processing we carry out, identify our legal basis for carrying it out and document it;

(7) ***Consent*** – we should review how we are seeking, obtaining and recording consent and whether we need to make any changes;

(8) ***Children*** – we should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity;

(9) ***Data breaches*** – We should make sure we have the right procedures in place to detect, report and investigate a personal data breach;

(10) ***Data Protection by Design and Data Protection Impact Assessments*** – We should familiarise ourselves with the ICO guidance on Privacy Impact Assessments and work out how and when to implement them;

(11) ***Data Protection Officer*** – We need to formally designate a Data Protection Officer who will take responsibility for data protection compliance and who will report directly to the highest levels of management within TMBC. At the moment this role is fulfilled on a day to day basis by the Director of Central Services & Monitoring Officer. If this post is to continue to perform the role in relation to the GDPR then a formal designation will need to be made;

(12) ***International*** – this applies if TMBC operates internationally and then we should determine which data protection supervisory authority we come under (not really applicable as we fall under the ICO).

1.4 The role of the Information Commissioner's Office (ICO)

1.4.1 The ICO has stated that it wants to help organisations understand the new legal framework in the EU. It will continue to issue guidance on aspects of the GDPR as we approach implementation.

1.4.2 The ICO is committed to assisting businesses and public bodies to prepare to meet the requirements of the GDPR ahead of May 2018 and beyond. They acknowledge that there may still be questions about how the GDPR would apply in the UK on leaving the EU, but this should not distract from the important task of compliance with the GDPR. With so many businesses and services operating across borders, international consistency around data protection laws and rights is crucial both to businesses and organisations, and to individuals. The ICO's role has always involved working closely with regulators in other countries, and that will continue to be the case. Having clear laws with safeguards in place is more important than ever given the growing digital economy, and the ICO will work with government to stay at the centre of these conversations about the long term future of UK data protection law and to provide advice where appropriate.

1.5 Recommendations

1.5.1 The work required to prepare for the GDPR (including the '12 steps' set out in paragraph 1.3.2) is being taken forward by the Information Governance Officer Steering Group, with input from appropriate colleagues from across the Council. For example, in reviewing our procedures for obtaining the consent of data subjects to the processing of their personal data, input has been obtained from several services across the Council.

1.5.2 Face to face training has already been provided to senior officers, with online training for all staff to be rolled out in advance of next May. It is intended that training will also be provided to all Councillors.

1.5.3 It is recommended that Members formally designate the Director of Central Services & Monitoring Officer as the Council's Data Protection Officer. In order to provide resilience it is further recommended that the Principal Solicitor and Principal Solicitor (Litigation) are both appointed as Deputy Data Protection Officers, so that they are able to perform the duties of the Data Protection Officer in the event that the Director of Central Services is unable to act in a particular case.

1.6 Financial and Value for Money Considerations

1.6.1 The financial considerations are set out above.

1.7 Legal Considerations

1.7.1 The legal considerations are set out above.

1.8 Risk Assessment

1.8.1 Compliance with the requirements of the GDPR is mandatory, so the Council needs to ensure it is fully prepared in advance of May 2018. The risks of non-compliance are set out in paragraph 1.1.3 above.

1.9 Equality Impact Assessment

1.9.1 None arising from this report.

1.10 Recommendation

1.10.1 It is **RECOMMENDED** that Members

(1) Note the contents of this report

(2) Appoint

a. the Director of Central Services & Monitoring Officer as the Council's Data Protection Officer;

b. the Principal Solicitor and Principal Solicitor (Litigation) as Deputy Data Protection Officers

contact: Adrian Stanfield

Background Papers:
None