Agenda Item No: 6 **Report No: 134/17**

Report Title: Preparation for Changes to Data Protection Legislation

Report To: Audit and Standards Committee Date: 25 September 2017

Wards Affected: All

Report By: Deputy Chief Executive

Contact Officer:

Name: Oliver Dixon
Post Title: Lawyer and Data Protection Officer
E-mail: oliver.dixon@lewes.gov.uk
Tel No: (01273) 085881

Purpose of Report:

To make the Committee aware of imminent changes to UK data protection legislation and how the Council is preparing for the higher standards of data privacy set by this new legal regime.

Officer Recommendations:

That Audit and Standards Committee–

(i) note the key features of the General Data Protection Regulation and the proposed Data Protection Bill; and

(ii) note the measures that Lewes District Council is taking to achieve compliance with the new legislation within the necessary timescale.

---

1. Reasons for Recommendations:

1.1 To fulfil its role in providing assurance of the adequacy of the Council's risk management arrangements, the Committee should satisfy itself that the Council is taking adequate steps to comply with the new data protection regime coming into force next year.

1.2 Non-compliance could expose the Council to significant financial penalties and reputational damage.

2. Information

Legal and Policy Background

2.1 For almost 20 years the Data Protection Act 1998, which gave effect to a 1995 European Union directive, has provided the legal framework for the use of personal data in the UK. Since that law was introduced the nature and use of data on individuals has undergone rapid and significant change, alongside new technologies for accessing and processing the information. Additionally, data protection laws have evolved differently across individual EU member states based on their own interpretation of the 1995 directive.

2.2 In response, the European Parliament have adopted a new **General Data Protection Regulation** ("GDPR") which comes into force across all EU member states in May 2018, replacing the 1995 directive and, in this country, the Data Protection Act 1998. The Government has confirmed that GDPR will continue to apply to the UK after Brexit, to enable business across the UK and EU member states to operate to the same high standards of data privacy and transparency, facilitating trade that relies on the flow of personal data.

2.3 The Data Protection Bill currently before UK Parliament will, when enacted, be the mechanism that ensures GDPR applies post Brexit. For further details of the Bill, see paragraph 2.7.

2.4 In addition to commercial benefits, the Government has identified two key reasons for adhering to GDPR:

(i) to engender confidence among the public that their personal data is safe and will be used responsibly; and

(ii) to maintain the ability of UK law enforcement bodies to share, receive and protect data with other EU member states in the fight against international crime.

GDPR - Key Provisions

2.4 Many of GDPR's main concepts and principles are much the same as those under the Data Protection Act 1998, with a focus on fairness, transparency, accuracy, security, minimisation and respect for the rights of individuals whose personal data we wish to process. However, there are new elements and significant enhancements to individuals' rights and the obligations on data controllers (bodies that decide how and why to collect data) and data processors (bodies that process data on behalf data controllers). For the most part, the Council is a data controller.

2.5 New or enhanced rights for individuals

2.5.1 Right to access their data. In addition to copies of the relevant data, individuals must be told how their data is being used, who it will be shared with, how long it will be kept and information on their other

rights as a data subject. In most cases this information must be supplied free of charge and within one month.

2.5.2 Right to be forgotten. Individuals will be entitled to have personal information about them deleted in certain circumstances. This right will not apply where it is necessary to retain the person's details in relation to legal proceedings, to comply with a statutory obligation, or to perform tasks in the public interest.

2.5.3 Data portability. A right for individuals to receive in a "structured, commonly used and machine readable" format any electronically held personal data, to enable transfer to another organisation. The individual can request the data controller to make this transfer free of charge.

2.5.4 Compensation. Any person who suffers financial or non-financial damage as a result of a data controller infringing GDPR will have the right to receive compensation from that controller.

2.6 <u>New or enhanced obligations on data controllers and processors</u>

2.6.1 Privacy notices. GDPR places great emphasis on controllers being transparent about the data they hold on individuals and communicating with them in clear language. The information that controllers must provide to individuals whose data are being processed is called a privacy notice. GDPR expands the contents of this notice to include controller identity, the purpose and legal basis for processing, the data retention period, which parties the data is shared with, and the individual's rights of data access etc. (as per para 2.5 above).

2.6.2 Consent. Controllers will not be permitted to rely on an individual's consent as the lawful basis for processing their data unless the consent is given clearly and affirmatively. Pre-ticked boxes signalling consent will not suffice.

2.6.3 Data Protection Impact Assessments. Where a controller wishes to process personal data that poses potentially high risks, they will have to carry out a data protection impact assessment in advance and take measures to mitigate the risks identified.

2.6.4 Accountability. Controllers must be able to demonstrate compliance with GDPR by fully documenting their data processing activities.

2.6.5 Data Protection Officer ("DPO"). Local authorities must appoint a DPO to inform and advise them on their obligations under the GDPR and to monitor compliance.

2.6.6 Data breach notification. Controllers must notify the Information Commissioner's Office ("ICO" – the UK regulator for data protection) within 72 hours of becoming aware of a data breach.

2.6.7 Penalties for data infringements. The ICO can issue warnings, reprimands, corrective orders and fines of up to 20 million euros (£17m) for breaching GDPR, a significant increase on the financial penalties available under the Data Protection Act 1998.

2.7 Data Protection Bill

2.7.1 The UK Government intends to introduce a Data Protection Bill in the current parliamentary year.

2.7.2 Although GDPR will automatically become law across the entire EU in May 2018, the Regulation allows each member state to provide exemptions from its obligations in very limited circumstances. This will make it lawful, for example, to process personal data on criminal convictions and offences where doing so is in the interests of public security. This is an important safeguard against potential criminal activity and will be provided for in the Bill.

2.7.3 The Bill will implement the Data Protection Law Enforcement Directive into UK law. This will enable public bodies with prosecution powers to share personal data for law enforcement purposes.

2.7.4 The Bill will create two new offences:

- an offence of intentionally or recklessly re-identifying individuals from anonymised data
- an offence of altering records with intent to prevent disclosure following a subject access request

2.8 Council Preparation

2.8.1 Most of the Council's preparation will involve enhancement to existing procedures and processes, rather than a complete overhaul. Some new arrangements will be necessary, though.

2.8.2 The Council has designated Oliver Dixon, Senior Lawyer, as its statutory DPO.

2.8.3 Transition to GDPR compliance is being project managed by a group of officers, with Alan Osborne as project sponsor. The DPO provides Corporate Management Team with regular updates on progress.

2.8.4 Work is underway to identify the Council's principal data processing activities so that any shortfall against the GDPR standard can be identified and put right.

2.8.5 The Council is already working with Civica on its Joint Transformation Programme and will use their digital expertise to advise on certain aspects of GDPR.

2.9 **Further Actions Required**

2.9.1 Review of privacy notices: is the information the Council gives to individuals about how it handles their data sufficient and transparent?

2.9.2 Review of consent forms: where individual consent to data processing is necessary, is it given to the Council clearly and affirmatively?

2.9.3 Review of data retention policy: is data held for the minimum period necessary and securely deleted thereafter?

2.9.4 Upgrade the breach notification policy: are we doing enough to detect data breaches; and if a breach is identified, is the internal and external notification procedure correct and fast enough?

2.9.5 Enhance the process for responding to individuals exercising their data rights, e.g. access to data, right to erasure. Is the Council geared to deal with requests within the shorter timeframe permitted? Does it have adequate and cost-effective data search and retrieval systems?

2.9.6 Officer training: serving officers need to be made aware of their stricter data obligations; and new recruits should not be given access to personal data until adequately trained.

2.9.7 Training for members in their personal capacity as data controllers when corresponding with ward constituents: do they know and comply with the new legal obligations?

2.9.8 All these actions will be scheduled for completion by the time GDPR comes into force in May 2018.

2.10 **Future reporting to Audit and Standards Committee**

2.10.1 In the unlikely event of a serious data breach at the Council, a report on the Council's response and recovery would be submitted to this Committee.

2.10.2 Any further significant changes to data protection legislation beyond GDPR and the Data Protection Bill may also be reported to this Committee for consideration, where the changes have serious risk implications.

3. Financial Appraisal

3.1 It is possible that the Council will need to procure new software to run sophisticated search and retrieval programmes against the personal data held by the Council in response to subject access requests and

requests for data erasure. The Head of Information Technology will identify system requirements and costs, to be funded from the corporate budget for Service Priorities.

3.2 The actions noted in this report mitigate the risk of a data breach and the associated potential cost of compensation and penalties.

4. Legal Implications

4.1 The most important legal aspects of GDPR and the proposed Data Protection Bill are dealt with in the body of the report.

4.2 The DPO will consider the Bill in detail when published and will track its course through Parliament until enacted as statute.

5. Risk Management Implications

5.1 Whilst the Council's strategic risk register does not make specific reference to data protection, the risk associated with new legislation generally, in terms of materially changing service requirements and standards, is recognised there.

5.2 Clearly there are very significant financial (see para 2.6.7) and reputational risks associated with a major data breach. However, the steps the Council is taking between now and May 2018, as detailed at paras 2.8 and 2.9, are designed to mitigate these risks substantially.

5.3 Internal Audit will review Council compliance with the general requirements of GDPR and will examine the extent to which the Council is likely to meet its new obligations under the Data Protection Bill. The initial review will be scheduled at an appropriate time during the Council's preparations for GDPR, and there will be a follow up study to confirm the action taken to address any issues noted by the initial review.

6. Background Papers

GDPR: Regulation (EU) 2016/679 of the European Parliament and of the European Council of 27 April 2016

'A New Data Protection Bill – Our Planned Reforms' (UK Government statement of Intent issued by DCMS 7 August 2017)