Broads Authority
29 September 2017
Agenda item No 15

General Data Protection Regulation
Report by Solicitor and Monitoring Officer

Summary:	This report provides a summary of important forthcoming changes to data law being implemented from 25 May 2018.
Recommendation:	That the Broads Authority notes the report.

1 Background

1.1 The law relating to the protection of data is currently contained in the Data Protection Act 1998 (DPA). Enforcement and guidance is provided by the Information Commissioner's Office (ICO).

1.2 From 25 May 2018 a significant change to data law will be implemented in the UK through the EU General Data Protection Regulation. Although there was some doubt as to whether this law change would take effect following the EU referendum, it has been clarified within the past few months that it will be implemented in full.

1.3 It was considered by the Financial Scrutiny and Audit Committee in July that Members should receive a briefing on the significance of the new changes.

2. Overview of legal changes

2.1 The changes and effects on the Authority include the following:

- Definition of data. This is much wider than current DPA and includes matters which could identify an individual such as genetic, mental or economic identity.
- As the new law increases complexity for data stored outside the EU, there will be a need to consider where data is stored. Officers believe that there is no "cloud storage" used by the Authority outside the EU, which would be the likely place for inadvertent breach.
- Consent is needed from a parent to process the data of children under 16. The tolls database may include the data of those from age 14.
- The processing of data will need explicit consent. Accordingly, there will be a greater need to obtain specific consents for data processing on forms and an outline of what the Authority will use the data for.

- By Article 35 of the GDPR, Data Protection Officers must be appointed for all public authorities. It is intended that the Monitoring Officer will take on this responsibility for the Broads Authority.

- Where there is higher risk data processing a risk assessment must be carried out. In terms of this, the Authority would look to ensure that its payroll and pensions information, which are administered by other authorities, are the subject of an assessment.

- There is a strict 72-hour self-reporting requirement for breaches and where the risk to individuals is high from a breach, they must be notified too. This means that there must be procedures in place for reporting up to the Data Protection Officer.

- The “Right to be forgotten” will be a key element of the new law as well as data portability. For compliance, it will be absolutely crucial that data is stored only on appropriate data sets.

- Where an authority processes data for another organisation, then it will be responsible for any breaches and vice-versa.

2.2 Of particular note is that penalties for serious breaches are up to €20,000,000.00 Euros or 4% of turnover. The current maximum is £500,000.00.

3 Implementation

3.1 The Management Team has implemented steps to ensure compliance with the new Regulation. A scoping group has identified a number of steps towards implementation and met on 4 August 2017. A Data Retention Policy is being drawn up by the Solicitor and Monitoring Officer identifying all categories of data and where it is held. This is hoped to be complete by the end of September 2017 in draft form. At that point the group will meet again and decide the next step towards implementation. This will focus on what consents are required for the future processing of data on each database and what changes are required for both electronic and printed forms. In addition which types of data processing will require risk assessments.

4 Conclusion and Recommendation

4.1 Members are invited to note the report.

Author: David Harris

Date of report: 15 September 2017

Appendices: None