REPORT OF:	**FINANCIAL SERVICES MANAGER**
TO:	**ACCOUNTS AND AUDIT COMMITTEE**
DATE:	**25th January 2018**

Contact Details:	Vince Green
Tel. No:	01282 661867
E-mail:	vince.green@pendle.gov.uk

General Data Protection Regulation (GDPR) – Progress Update

PURPOSE OF REPORT

The purpose of this report is to update the Committee on the progress made within the Council in response to the General Data Protection Regulation (GDPR). The GDPR replaces the long-standing Data Protection Act (DPA) in May 2018.

RECOMMENDATIONS

The Committee is recommended to note the application of the General Data Protection Regulation with effect from 25th May 2018 and the work carried out both to-date and planned in the near term to enable the Council to comply with the regulation.

REASONS FOR RECOMMENDATION

To ensure the Committee is aware of the implications of GDPR and the work being implemented to achieve corporate compliance.

ISSUE

1. ***What is the General Data Protection Regulation (GDPR)?***

1.1. GDPR is an EU regulation which is intended to strengthen and unify data protection for all individuals within the European Union. It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

1.2. When the GDPR takes effect, it will replace the EU Data Protection Directive of 1995 which gave rise in the UK to the 1998 Data Protection Act. The GDPR becomes enforceable from 25 May 2018 after a two-year transition period and, unlike a directive, it does not require national governments to pass any enabling legislation, and is thus directly binding and applicable. The government has confirmed that the decision to leave the EU will not affect the commencement of the GDPR in the UK.

2. ***Who does the GDPR apply to?***

2.1. The GDPR applies to data 'controllers' and 'processors'. The definitions are broadly the same as under the DPA – i.e. the controller says how and why personal data is processed and the processor acts on the controller's behalf. The GDPR places specific legal obligations on processors; for example, the requirement to maintain records of personal data and processing activities. There is significantly more legal liability if a processor is responsible for a breach. These obligations for processors are a new requirement under the GDPR.

2.2. However, controllers are not relieved of their obligations where a processor is involved – the GDPR places further obligations on controllers to ensure any contracts with processors comply with the GDPR. This has implications for the Council's arrangements with Liberata and potentially a wider range of partners. The Council will act as both controller and processor in relation to GDPR.

3. ***What information does the GDPR apply to?***

Personal data

3.1. Like the DPA, the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – e.g. an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

3.2. For most organisations, keeping HR records, customer lists, or contact details etc, the change to the definition should make little practical difference. If we hold information that falls within the scope of the DPA, it will also fall within the scope of the GDPR.

3.3. The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This is wider than the DPA's definition and could include chronologically ordered sets of manual records containing personal data.

3.4. Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data

3.5. The GDPR refers to sensitive personal data as "special categories of personal data". These categories are broadly the same as those in the DPA, but there are some minor changes. For example, the special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

4. ***Data Protection Principles***

4.1. Under the GDPR, the data protection principles set out the main responsibilities for organisations. The principles are similar to those in the DPA, with added detail at certain points and a new **accountability** requirement. The GDPR does not have principles relating to individuals' rights or overseas transfers of personal data - these are specifically addressed in separate articles. The most significant addition is the accountability principle. The GDPR requires us to show **how** we comply with the principles – for example by documenting the decisions we take about a processing activity. Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

4.2. The principles are reproduced at **Appendix A**.

5. The implications of GDPR for the Council are widespread and potentially significant. We will need to have consent or one of five other specific legitimate reasons to hold and process individuals' data, including all legacy data. The GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

The above obligations apply to both data controllers and data processors.

6. There is a lot of external information, guidance and sales/consultancy services available in the run up to the implementation deadline. An authoritative source of information/guidance is the ICO website (https://ico.org.uk/for-organisations/data-protection-reform/). The ICO has published a booklet to help organisations prepare for GDPR entitled "Preparing for GDPR – 12 steps to take now".

7. An initial report outlining the implications of GDPR was considered by Management Team last Autumn and this identified the following as the main actions based on the ICO guidance:

- Raising organisational awareness;
- Documenting what personal data we hold;
- Review of current privacy notices and updating in time for implementation;
- Assessing and implementing / refining processes to ensure we can respond appropriately when individuals exercise their rights as set out in 5 above;
- Identifying the lawful basis for our processing of personal data;
- Review how we seek, record and manage consent;
- Designate someone to take responsibility for data protection compliance and assess where this role sits in our structure and governance arrangements.

Overview of actions taken to-date

8. Awareness of GDPR has been raised via a report to Management Team, followed by a presentation to service managers. Further communications have been developed for all staff and consideration is being given to what other forms of communication and training may be beneficial prior to implementation (e.g. e-learning module).

9. One of the key packages of work is to gather a detailed understanding of what information the Council currently holds. This is a significant task given the range of services and levels of information held. This also extends to the Council's contractual arrangements with Liberata and other providers who may process or control information on behalf of the Council.

10. In support of this activity an on-line data capture form has been developed for services to complete and the deadline for this action is the 19th January. The information gathered from this exercise will help establish such matters as:

- Who is the data controller / processor
- The lawful basis for processing personal data
- Where and what format information is held and for what purpose
- How customers are informed of our use of data and who it may be shared with
- When and how consent is obtained
- The approach to the retention and disposal of information.

11. In addition to the above, the following actions are planned in the near term:

    - review and amend as necessary the procedure for dealing with Subject Access Requests – such requests will be free of charge under GDPR and we will have one month rather than 40 days as now to respond;

    - review and update as required the Council's privacy notice to ensure compliance with GDPR;

    - reviewing our approach to data protection impact assessments to ensure data protection considerations are reflected appropriately in the design of any new or revised system/application.

    - updating our contractual arrangements with 3rd parties who process data on our behalf to ensure the requirements and obligations of GDPR are reflected appropriately;

    - ongoing communications, information and awareness raising for staff;

    - establishing a data/document retention policy adapting a template developed by the Local Government Association for this purpose.

12. This work is overseen by a small group of officers supported by representatives from various service departments.

IMPLICATIONS

Policy

13. There will be policy implications arising from the work required to implement GDPR and these will be addressed as part of the work programme. Policies linked to data protection, data retention and disposal as well as other IT related policies will most likely fall within the scope of this activity.

Financial

14. There is no budget provision for GDPR. Every effort is being made to progress the work within existing resources but where this is not possible the report author will update Management Team accordingly and look to secure budget provision utlising the flexibility provided in the Council's Financial Procedure Rules.

Legal

15. The GDPR contains various mandatory requirements which the Council must comply with.

Risk Management

16. There are potentially significant risks associated with GDPR including significant financial risk in the event of fines for non-compliance as well as reputational risk in the event of a breach or our inability to meet the rights of individuals effectively.

Health and Safety

17. There are no health and safety implications arising from the contents of this report.

Climate Change

18. There are no climate change implications arising directly from the contents of this report.

Community Safety

19. There are no community safety issues arising from the contents of this report.

Equality and Diversity

20. There are no equality and diversity implications arising from the contents of this report.

APPENDICES

Appendix A – GDPR Data Principles

APPENDIX A – GDPR DATA PRINCIPLES

Article 5 of the GDPR requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."