Committee:	**Governance, Audit and Performance**	**Agenda Item**
Date:	**16 November 2017**	**7**
Title:	**General Data Protection Regulation (GDPR) Implementation**	
Author:	**Sheila Bronson, GDPR Project Lead Officer 01799 510610**	Item for information

Summary

1. To report to the Governance, Audit & Performance Committee details of work being undertaken by the Council towards compliance with the EU General Data Protection Regulation (GDPR) which will come into force on 25 May 2018.

Recommendation

2. That the General Data Protection Regulation Report be noted.

Financial Implications

3. None

Background Papers

4. None

Impact

5.

Communication/Consultation	An officer Project Team has been set up with representation from all departments. A communication strategy will be a key part of implementing the GDPR.
Community Safety	none
Equalities	None direct, although the need to protect sensitive personal data may be more significant for groups with one or more protected characteristics.
Health and Safety	none
Human Rights/Legal Implications	The Council is under a legal obligation to comply with the terms of the GDPR when

	they take effect on 25 May 2018. Penalties can be imposed, and reputational damage suffered, if it does not. Non-compliance may also lead to an infringement of the rights of individuals, in particular their "Article 8" right to respect for their private life and home.
Sustainability	none
Ward-specific impacts	none
Workforce/Workplace	All Council employees need to be aware of data protection requirements and to carry out their work in a compliant manner. This is particularly important for employees who have access to sensitive personal information about members of the public.

Situation

6. The EU General Data Protection Regulation (GDPR) come into force on 25 May 2018.

7. GDPR will replace the Data Protection Act 1998, and will be supplemented by the Data Protection Bill 2017-19 currently progressing through Parliament.

8. GDPR extends the obligations on the Council and makes additional requirements. These include:

    - A new **"integrity and confidentiality principle"**. This states that personal data must be "processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organisational measures".

    - Keeping a **detailed record of processing operations**. The requirement in current data protection laws to notify the Information Commissioner about data processing operations is abolished and replaced by a more general obligation on the Council to keep extensive internal records of its data protection activities.

    - Performing **data protection impact assessment** for high risk processing. This is processing which is likely to result in a high risk to the rights and freedoms of individuals; for example automated processing that significantly affect individuals or processing of sensitive personal data.

    - Notifying and keeping a **comprehensive record of data breaches.**

- Implementing data protection by **"design and by default"**. This means assessing carefully and implementing appropriate technical and organisational measures and procedures from the outset to ensure that processing complies with GDPR and protects the rights of the data subjects. It also means ensuring mechanisms are in place within the Council to ensure that, by default, only personal data which are necessary for each specific purpose are processed. This obligation includes ensuring that only the minimum amount of personal data is collected and proessed for a specific purpose; the extent of processing is limited to that necessary for each purpose; the data is stored no longer than necessary and access is restricted to that necessary for each purpose.

9. GDPR also gives enhanced rights to individuals. These rights are backed up with provisions making it easier to claim damages for compensation and for consumer groups to enforce rights on behalf of consumers. These include:

    - **Transparency.** Specified information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language.
    - **Subject access rights.** These are similar to the current provisions, although enhanced in some respects and there is no longer a general right to charge a fee. Information requested by data subjects must be provided within one month as a default with a limited right for the controller to extend this period for up to three months.
    - **Right to rectify.** Similar to current provisions - a right to require inaccurate or incomplete personal data to be corrected or completed without undue delay.
    - **Right to erasure ('right to be forgotten').** The scope of the right to erasure is very limited but is linked to the obligation of the Council to delete data that it no longer needs.
    - **Right to data portability (Article 20).** This is an entirely new right in GDPR and has no equivalent in the current Directive. Where the processing of personal data is justified either on the basis that the data subject has given their consent to processing or where processing is necessary for the performance of a contract, or where the processing is carried out be automated means, then the data subject has the right to receive or have transmitted to another controller all personal data concerning them in a structured, commonly used and machine-readable format.

10. An additional complication for the Council is that the lawful grounds for processing personal information are changed. The requirements are much more rigorous where the Council relies on the consent of the data subject. The Council, also, cannot rely on its "legitimate interests" to process data. It will need to examine the data it holds and the lawful basis for processing. Where it is not relying on consent, it will have to identify the justification for processing. Fortunately, these are quite widely drawn and in most cases the

Council will be able to rely on the ground that “processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.”

11. The Information Commissioner will have the power to impose sanctions varying in severity from warnings; reprimands and corrective orders to fines of up to €20m should the Council be unable to demonstrate GDPR compliance in the event of a data breach.

12. The Council has established a GDPR Project Team to undertake a programme of work to review the Council’s current level of compliance and the actions needed to ensure gaps in compliance are rectified by 25 May 2018.

13. Two temporary posts (12 months) have been created to oversee the GDPR compliance work; with the Internal Audit Manager appointed as GDPR Lead Officer and a GDPR Compliance Officer expected to take up his post on 13 November 2017.

Work Programme

14. The Information Commissioner has published guidance on the twelve principal steps that organisations should take to ensure GDPR compliance. These are appended to this report and form the basis of the Council’s work programme.

15. An initial Data Survey of senior management has been undertaken from which a Data Inventory is being compiled.

16. A GDPR Project Plan has been drawn up and milestones agreed.

17. A Council wide data mapping and flowcharting exercise will commence shortly, prioritising the services which gather and process the highest volume of personal data. This exercise will identify the areas where further action is required to ensure compliance.

18. Further action is set out in the Project Plan to address the twelve steps identified by the Information Commissioner. The Project Plan will be kept under review and adapted as further guidance becomes available and as the Data Protection Bill proceeds through Parliament. Regular updates are scheduled to report to the Corporate Management Team.

Update on Progress

19. GDPR Compliance Progress Reports will be brought to future meetings of this committee during the lifetime of the GDPR Project.

Risk Analysis

20.

Risk	Likelihood	Impact	Mitigating actions
The Information Commissioner can impose sanctions on the Council if it fails to show its compliance with GDPR from 25 May 2018	1 The Council may not achieve full compliance by 25 May 2018	3 Data breeches due to non-compliance will be subject to sanctions varying in severity from warnings, reprimands, corrective orders to fines of up to €20m	Action is being taken to towards ensuring the Council is in a position to demonstrate GDPR Compliance by 25 May 2018

1 = Little or no risk or impact
2 = Some risk or impact – action may be necessary.
3 = Significant risk or impact – action required
4 = Near certainty of risk occurring, catastrophic effect or failure of project.

Appendix

Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now (Published by the Information Commissioner's Office.)

1. Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have. Implementing the GDPR could have significant resource implications, especially for larger and more complex organisations. You may find compliance difficult if you leave your preparations until the last minute.

2. Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3. Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4. Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5. Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6. Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7. Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8. Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9. Data breaches

You should make sure you 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

You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11. Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12. International

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this**.**