Update on GDPR for November 2017 Audit and Standards Committee

The General Data Protection Regulation (GDPR), which is to replace the Data Protection Act (DPA), will be implemented on 25 May 2018. It is crucial that the Council is prepared for it, not least because the fines for non-compliance have increased substantially.

The focus of the new legislation is on greater proactivity and transparency. The Council will need to be clear about the information it holds, ensure that there is a proper legal basis for holding it and that individuals' consent has been obtained. Consent for personal data to be processed must be "freely given, specific, informed and unambiguous" – a pre-ticked box will no longer be adequate.

Among other provisions, the GDPR expands the definition of personal data to cover, for example, location, cookies and IP addresses. It introduces new concepts including "sensitive data" such as biometric information (for example photographs would qualify as biometric data if processed through a specific technical means allowing the unique identification or verification of a person's identify). For sensitive data, consent must be explicit. In the case of a challenge, the onus will be on the Council to demonstrate that consent was given.

Subjects of the data will have new rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

A brief overview of these rights follows.

1. <u>The right to be informed</u>

   The GDPR sets out the information that the Council should supply and when individuals should be informed. The information to be supplied is determined by whether or not the personal data was obtained directly from individuals. Much of this information is consistent with current obligations under the DPA, but there is some further information the Council will be explicitly required to provide. The information about the processing of personal data must be:

   - concise, transparent, intelligible and easily accessible;
   - written in clear and plain language, particularly if addressed to a child; and
   - free of charge.

2. The right of access

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information.

These are similar to existing subject access rights under the DPA.

However, this information must be provided free of charge. The removal of the £10 subject access fee is a significant change from the existing rules.

3. The right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If the Council has disclosed the personal data in question to third parties, it must inform them of the rectification where possible. It must also inform the individuals about the third parties to whom the data has been disclosed.

A response must be given within one month (more quickly than the current 40 days).

4. The right to erasure

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Under the DPA, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under the GDPR, this threshold is not present.

5. The right to restrict processing

The Council will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data (the processing must be restricted until the accuracy of the data has been verified);
- Where an individual has objected to the processing and the Council is considering whether it has legitimate grounds that override those of the individual;
- When processing is unlawful and the individual opposes erasure and requests restriction instead;
- If the Council no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

6. The right to data portability

   The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

7. The right to object

   Individuals have the right to object particularly with regard to direct marketing and processing for purposes of scientific or historical research and statistics.

8. Rights in relation to automated decision making and profiling.

   The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. It will be important to identify whether any of the Council's processing operations constitute automated decision making and consider whether procedures need to be updated to deal with the requirements of the GDPR.

The Plan

A project team has been created to lead on this issue and consists of colleagues from Legal Services, Insurance, Internal Audit and IT. The team has been talking to Heads of Service and service managers to identify all systems used across the Council and each service has completed an Information Asset Register.

Moving forward, the project team will be identifying how and why personal data is collected and used to ensure this meets GDPR. The relevant Council policies and procedures will all need to be updated, including the Document Retention Policy. Services will need to identify and securely destroy any personal data that it no longer needs.

Compulsory WISENET training is being developed for all colleagues to complete and will help Officers understand how the GDPR affects individuals and the Council as a whole, and how they can assist the Council to comply.

The GDPR also sets strict timescales for reporting a data breach to the Information Commissioner's Office (ICO). Where there is a risk to an individual, it must be reported within 72 hours of becoming aware of the breach. Examples of a breach are the sending of personal data to the wrong recipient or the loss of a laptop or work phone containing personal information. Staff have been reminded of the Council's Data Security Breach Management Policy.
As the project plan is delivered there will be regular updates in the staff newsletter (WIS) and GDPR 'Frequently Asked Questions' area developed on the infonet.