Preparing for the General Data Protection Regulation (GDPR) - overview

Awareness

- Decision makers and key people in the organisation need to be aware that the law is changing. https://ico.org.uk/for-organisations/data-protection-reform/gdpr-messages-for-the-boardroom/
- New procedures required to deal with the GDPR's new transparency and individuals' rights provisions.
- Greater emphasis on the documentation that data controllers must keep to demonstrate their accountability.

Information held

- Need to document what personal data the council holds, where it came from and who it is shared with.
- Inaccurate information must be updated and notified to anyone the data has been shared with.

Communicating privacy information

- Current privacy notices should be reviewed and a plan put in place for making any necessary changes in time for GDPR implementation.
- New privacy notices must be created where none exist
- Clear, easy to understand language must be used.
- https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

Individuals' rights

Procedures must be checked to ensure they cover all the rights individuals have, including how personal data would be deleted or provided electronically and in a commonly used format.

The main rights for individuals under the GDPR will be:

- subject access,
- to have inaccuracies corrected,
- to have information erased,
- to prevent direct marketing,
- to prevent automated decision-making and profiling, and
- data portability.

Subject access requests

- New timescale – one month to reply unless complex.
- Notify of refusal or need for extension within one month.
- Manifestly unfounded or excessive requests can be charged for or refused.
- Need policies and procedures in place to detail grounds for refusal
- Additional information must be provided.

Legal basis for processing personal data

The council should look at the various types of data processing it carries out, identify the legal basis for carrying it out and document it. The council will also have to explain the legal basis for processing personal data in its privacy notice and when answering subject access requests.

Consent

- Check how the council seeks, obtains and records consent
- Make necessary changes and ensure consent can be demonstrated
- Consent must be positive agreement to personal data being processed – it cannot be inferred from silence, preticked boxes or inactivity.
- Put systems in place to ensure consent can be withdrawn

Children

- Put systems in place to verify individuals' ages and to gather parental or guardian consent for data processing

- If the council collects information about children – in the UK anyone under 13 – then a parent or guardian's consent will be required in order to process their personal data lawfully.
- The relevant privacy notice must be written in language that children will understand.

Data breaches

- Risk assessment process must be followed
- Only 72 hours to decide if a breach needs to be reported to the ICO.
- Individuals may need to be told too if they are likely to suffer some sort of damage.
- Failure to report may lead to a fine in addition to the fine for the breach itself
- Increased fines – up to the higher of 4% of annual worldwide turnover and EUR20 million

Data Protection by Design and Data Protection Impact Assessments

Relevant council officers should familiarise themselves with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them within the council. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

- Assess situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally?
- Note that you do not always have to carry out a DPIA - only in high-risk situations, for example where a new technology is being deployed or where a profiling operation is likely to significantly affect individuals.
- Introduce procedures for consulting the ICO to seek its opinion as to whether the processing operation complies with the GDPR if the council assess a project as being high risk.

Data Protection Officer

A Data Protection Officer (DPO) must be appointed.

Data Protection Bill

Following on GDPR, this Bill will update existing data protection legislation in the UK. **https://services.parliament.uk/bills/2017-19/dataprotection.html**

First reading took place on 13 September. This stage is a formality that signals the start of the Bill's journey through the Lords.

Second reading - the general debate on all aspects of the Bill - is scheduled for 10 October.