GENERAL DATA PROTECTION REGULATIONS

New Legal Framework:

- EU regulation, effect on 25 May 2018
- Commencement of GDPR not effected by Brexit
- Data Protection Act 1998 due to be repealed by 25 May 2018
- Data Protection Bill (to incorporate GDPR) due to be enacted by 25 May 2018

GDPR

- Designed to address the use of personal data in a technological/global age
- Retains existing legal principles in DPA 1998
- Retains key definition in DPA 1998, eg data controller, data processor, processing, personal data
- Builds on existing obligations in DPA 1998 re data controllers and individuals rights
- Good practice under DPA 1998 converted to statutory obligations under GDPR, eg privacy impact assessments
- Increases obligations on data processors

Six principles for processing personal data: (**bold – differences to DPA 1998)**

1. processed lawfully, fairly and in a **transparent** manner in relation to the individual/data subject
2. collated for specified, **explicit** and legitimate purpose(s)
3. adequate, relevant and limited to the purpose(s) for which they are processed
4. accurate and up-to-date; **inaccurate data shall be erased or rectified without delay**
5. kept for no longer than necessary for the purpose(s) for which it was processed and
6. secure, using appropriate technical or organisation measures

GDPR – when is it lawful to process personal data?

- The data subject has given **consent** to the processing of his personal data for specific purpose(s)
- Necessary for the performance of a contractual obligation with an individual or in order to take steps at the request of an individual prior to entering into a contract (**ie contractual necessity)**
- Necessary for compliance with the data controller's **legal obligations** (ie not contractual)
- Necessary to protection the data subject or another individual's vital interests (eg in a medical emergency)
- Necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller

GDPR – What about sensitive personal data?

Racial or ethnic origin, political opinions, religious or **philosophical beliefs**; trade union membership, **genetic data, biometric data for the purpose of uniquely identifying an individual**, health and sex life or sexual orientation

GDPR – when is it lawful to process sensitive personal data?

- If the data subject has given explicit consent to the processing for specified purpose(s)
- If necessary for carrying out the controller's or individual's rights and obligations in employment, social security law etc
- If it relates to personal data manifestly made public by the individual (eg on their own social media account, put in the public domain by the individual no need for explicit consent)
- If necessary for legal proceedings
- If necessary for assessing the working capacity of an employees (ie processing medical or occupational health data)

FAIR PROCESSING: Organisations must be transparent/clear and open with individuals about how their information will be used.

This is achieved by …. **Privacy notices**

GDPR - Privacy Notices – must provide a set of information which includes:

- The identity and the contact details of the data controller and, where applicable the data processor
- The contact details of the DPO
- The purposes of the processing (eg to maintain accounts and records; to recruit and manage staff, manage premises, crime prevention)
- The legal basis for the processing (eg consent, contractual obligations, statutory or other legal obligations)
- The recipients of the personal data (if any)(e.g. credit reference agencies, HMRC, pension providers)
- The period of which the personal data will be stored (if that's not possible, the criteria used to determine that period)
- Information about individual's statutory rights in respect of their personal data, eg the right to complain to the ICO

GDPR – What's new?

- Detailed privacy notices
- New approach to relying on consent for processing (how to get it and document it)
- New duty to report data breaches (within 72hrs to ICO)
- Responding to subject access requests – generally within 1 month and cannot charge fee
- More rights for individuals eg including right to be erased/forgotten
- New duty to keep internal register of processing activities
- Privacy impact assessments in respect of activities to be determined by ICO (not required in every activity – more information from ICO)
- New duty to appoint a Data Protection Officer (DPO)
- Robust contracts between data controllers and processors

Data controllers need **detailed contracts** with data processors to confirm eg

- What the processor can or cannot do with personal data
- That processor will keep personal data secure
- Notify the data controller of a personal data breach
- Return/delete personal data at end of contract
- Will assist controller with requests from individuals concerning rights of access, to rectify and object to processing of personal data
- Will assist controller with privacy impact assessments
- Processor will demonstrate compliance with contractual obligations

New obligations on data processors, eg

- To appoint a DPO
- To notify data controller of data breaches
- To keep internal record of processing activities

- High fines for data controllers and data processors
- ICO may use range of measures to respond to data breaches – warnings, reprimands, corrective orders and fines
- 2 levels of fines, either up to 10 million Euros (eg failure to appoint a DPO, to report breaches, to maintain written records for processing activities, in relation to the conduct of privacy impact assessments) or 20 million Euros (eg failure to observe principles for processing including conditions for consent or data subjects rights)

The Data Controllers obligations under the GDPR are:

Working with Data Processors

Privacy notices

- Fair processing of personal data involves transparency and providing information – in the form of a privacy notice
- GDPR requirements more detailed than current DPA regime – emphasis on making privacy notices understandable and accessible
- Information to be provided by data controller council in a privacy notice must be: concise, transparent, intelligible and easily accessible; written in clear and plain language (particularly if addressed to a child) and free of charge
- Information that must be provided by council in privacy notice depends on whether data is obtained directly from data subject or not

Privacy notice content:

- to help council decide what it needs to include it should work out: what information it holds that constitutes personal data; what is the purpose of the processing; what it actually needs to carry out these processes

Keeping internal records

- Councils must put in place comprehensive and proportionate governance measures
- Councils must maintain internal records of processing activities including name of organisation, purpose of processing, description of the categories of individuals and categories of personal data – similar to DPA requirement for data controllers to notify with the ICO
- Councils will be required to carry out Data Protection Impact Assessments in cases of potentially high-risk processing activities and to consult the ICO in certain instances, eg for high- risk processing operations

Reporting breaches:

- Duty on all organisations to report certain types of data breach to ICO and where a breach is likely to result in a high risk to the rights and freedoms of individuals, to notify data subjects concerned directly
- Personal data breach – breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data (eg publishing photographs from which individuals can be identified on councils website) NB – more than just losing personal data
- Only have to notify ICO of breach where it is likely to result in a risk to individuals' rights (eg lost paper files containing employee NI numbers)
- Council should notify DPO of data breaches

DPO appointment:

Responsibilities

- to understand the nature, scope, context and purposes of PC's processing activities and associated risks
- to be involved in PC's decisions/activities which have data protection law implications
- to inform, advise and make recommendations to PC
- to analyse and monitor PC's compliance with data protection law
- to raise awareness of data protection law with councillors and staff
- to directly report to the "highest management level" ie full council
- to assist PC in carrying out privacy impact assessments
- to conduct audits of legal requirements, practices and procedures
- to be contact for ICO
- to be contact for data subjects (eg employees, local residents, allotment tenants)
- to be consulted by PC if data breach has occurred

Qualifications - DPO expected to have **"professional qualities and expert** knowledge of **data protection law and practices"** proportionate to the type of processing that PC carries out, taking into consideration the level of protection required for personal data AND should have an understanding of PC's administrative rules and procedures

Resources - Must have:

- Support for DPO function by senior management, ie full council
- Co-operation by staff
- Sufficient time and resources (eg premises, facilities, equipment, staff) to perform his tasks
- Continuous training to maintain expert knowledge of data protection law and practice
- Access to services/teams/staff/committees within PC so DPO can receive essential information and support from them
-

WHO CAN BE DPO?

- May be an employee or a contractor
- If DPO is a contractor, various options exist eg a person may be a DPO to several PCs/other local authorities or organisations

CLERK/RFO AS DPO?
A DPO needs the following:

- Expert knowledge of data protection law and practices
- Adequate time to perform DPO role
- Integrity/professional ethics to effectively advise and influence PC
- **Independence** (ie not taking instructions from PC about exercising DPO's tasks and not at risk of dismissal from PC for performing DPO's duties)
- **no conflict of interests** (arising from clerk/RFO's responsibilities)

GDPR – Consent

What is consent?
"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

What is "freely given"?

- genuine and free of choice
- should be able to withdraw consent without detriment

Consent and the contract of employment
"for the purposes of the Data Protection Act 1998 you consent to the processing of all or any personal data (including sensitive personal data) in manual, electronic or any other form relevant to your employment. Processing includes but is not limited to obtaining, recording, using and holding data"

- can't be imbalance between the individual and the data controller

What is "specific, informed and unambiguous"?

- individual must be aware of the identity of the data controller and the purposes of the processing
- consent must be for each and every purpose
- must leave no doubt as to the individual's intention to consent

What is “affirmative action”

- must be a positive opt-in
- need not be explicit
- consent can be inferred from some actions but cannot be inferred from silence, pre-ticked boxes or inactivity

What is “explicit consent”?

- requires very clear, informed and specific statement of consent
- must be expressly confirmed in words
- can be oral but written is probably better
- cannot be by action

Asking for consent

- Is request for consent prominent and separate from other terms?
- Is there an opt-in?
- Are there no pre-ticked boxes?
- Is consent in “plain English”?
- Is it clear why data is wanted and what will be done with it?
- Is consent granular? (specific rather than in general terms)
- Is organisation named?
- Is withdrawal of consent clearly “flagged”?
- Is refusal to consent protected?
- Has consent been made a precondition of a service?
- Is consent appropriate basis for processing personal data?

Recording consent

- Are details of consent recorded?
- Are details of what data subject told recorded?

Managing consent

- Have consents been checked for changes?
- Is there a process for renewing consent?
- Have good practices been adopted, eg privacy dashboard?
- Is it easy to withdraw consent?
- Is withdrawal of consent without repercussions for data subject?

Examples:

- A council’s mailshot contains a tick box to be placed on a mailing list for specified community events
- At a council run event participants are individually asked for permission to use personal data the next time the council holds such an event
- A council website requires residents to provide personal data to access a particular part of it. There is a notice in that part which states that, by accessing it, they have consented to the data being processed by third parties
- Tickets for a council run event state that photographs will be taken and may appear on the council’s website
- A contract with an individual contractor requires her agreement that personal data will be put on the council’s website

Individuals rights under GDPR

GDPR creates new rights for individuals and strengthens existing rights under DPA

Rights for individuals under GDPR:

- The right to be informed
  - Data controller council must provide fair processing information (ie through a privacy notice)
  - Right emphasises the need for transparency on use of personal data
  - Content of privacy notice (more information on ICO website)

- The right of access
  - Similar to existing subject access requests under DPA
  - Individuals will have the right to obtain confirmation their data is being processed, access to their personal data and other supplementary information
  - Purpose of right? So individuals are aware of and can verify the lawfulness of the processing of their personal data
  - Copy of the information must be provided free of charge – removal of £10 subject access fee under DPA BUT – reasonable fee can be charged when a request is manifestly unfounded or excessive or repetitive and to comply with requests for further copies of the same information
  - Fee must be based on the administrative cost of providing the information
  - Length of compliance? Information must be provided without delay and at the latest within one month of receipt – **NB shorter time frame than DPA**

- The right to rectification
  - Right for individuals to have personal data rectified if it is inaccurate or incomplete
  - If the personal data has been disclosed to third parties, council must inform them of the rectification where possible. Relevant individuals must also be informed about the third parties to whom the data has been disclosed where appropriate
  - Response time for compliance with a request for rectification? One month – can be extended by two months where the request for rectification is complex
  - Where a council is not taking action in response to a request for rectification, must explain why to the individual, informing them of their right to complain to the ICO and to a judicial remedy

- The right to erasure/right to be forgotten
  - Right does not provide an absolute right to be forgotten
  - Individuals have a right to have personal data erased and to prevent processing in specific circumstances
  - Right applies:
    - Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed (eg unsuccessful job applicants)
    - When the individual withdraws consent (eg mailing list for council newsletter)
    - When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing (eg councillors' postal addresses details on website)
    - Where the personal data was unlawfully processed

    - Where the personal data has to be erased in order to comply with the legal obligation

- The right to restrict processing
  - The councils will be required to restrict the processing of personal data …
    - Where an individual contests accuracy of personal data, council should restrict the processing until accuracy of the personal data has been verified
    - Where an individual has objected to processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests) and council is considering whether organisation's legitimate grounds override those of the individual
    - When processing is unlawful and the individual opposes erasure and requests restriction instead
    - If council no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

    Council may need to review procedures to ensure it is able to determine where it may be required to restrict the processing of personal data
  - If council has disclosed the personal data in question to third parties, it must inform them about the restriction on the processing of the personal data, unless it is impossible or involved disproportionate effort to do so
  - Council must inform individuals when it decides to lift a restriction on processing

- The right to data portability
  - Right allows individuals to obtain and reuse their personal data for their own purposes across different services
  - Allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way (eg council changing its bank account)
  - Right only applies:
    - To personal data an individual has provided to a data controller council
    - Where the processing is based on the individual's consent or for the performance of a contract
    - When processing is carried out by automated means
  - Council must respond without undue delay and within one month – can be extended (by two months)
  - Where council is not taking action in response to a request, must explain why to the individual, informing them of their right to complain to the ICO and to a judicial remedy without undue delay and at the latest within one month

- The right to object
  - Individuals have the right to object to specific processing purposes
  - One example – direct marketing – eg council owns a theatre and uses database of individuals that previously bought tickets to a show to email them to promote new pantomime. Council would be using data without individuals' consent to it being processed in that manner

- Rights in relation to automated decision making and profiling
  - Individuals have the right not to be subject to a decision when it is based on automated processing and it produces a legal effect or a similarly significant effect on the individual

- Council must ensure that individuals are able to obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it

GDPR COMPLIANCE

First Steps

- Data clear out – why is council collecting data
- Specific purpose
- Digital **and** manual data
- Existing contracts

Map your Data

Questions to ask:

- How sensitive is the data (personal, sensitive, anonymous)?
- Where does it come from?
- Where is it kept?
- Where does it go within council and who has access to the data?
- Is it shared with any third party?
- How is it transferred?

Review Data Security

- Are there adequate firewalls and virus protections?
- Is there a clear password policy? Is it enforced?
- Encryption
- Storage
- Is there a procedure for managing a data breach? Who is responsible for it? Do all staff understand the procedure?

Implement new processes

- Consent – if appropriate
- Privacy notices – must be clear
- Data retention policy
- SAR process
- To implement new rights
- Breach reporting process
- Staff/councillor training
- Data Protection Officer