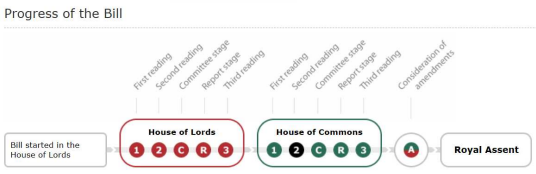
Data Protection Act 2018 (Including GDPR)

DPA 18 Summary

- It will replace & repeal the Data Protection Act 1998
  - Expected before 25 May 2018
- GDPR implementation will be a main feature of the act
  - Over 75 changes to the original GDPR text
- UK derogations have been decided
- New criminal offences will be created
  - Intentionally or recklessly re-identifying individuals from anonymised or pseudonymised data.
  - Altering records with intent to prevent disclosure following a subject access request.
- A more prescriptive logging requirement so a full audit trail will be available for adding, changing & deleting data.
- Additional definitions of personal data including Biometrics, IP Addresses & cookies
- It will also implement the Data Protection Law Enforcement Directive



What does it mean for you?

- The act empowers citizens to be more in control of their data
- You will be able to decide who processes and stores data about you
- Websites will have to stop marketing things to you based on previous history
- You will be able to request a copy of your data free of charge from any organisation
- In some cases they will have to supply your information electronically
  - This will allow you to move service easily, for example moving from one streaming music services to another and being able to keep the same playlists.
- You will be able to ensure that a marketing company erases your data if you want to stop them contacting you
- You will have greater guarantees that your data is being protected

DPA Principles

- **It covers the same aspects as the current DPA in 6 principles instead of 8**
  - 1. Processed fairly, lawfully and in a transparent manner
  - 2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with the original purpose
  - 3. Adequate, relevant and limited to what is necessary in relation to the purposes
  - 4. Accurate and kept up to date
  - 5. Kept in a form that permits identification no longer than is necessary
  - 6. Processed in a way that ensure appropriate security of the personal data
- However an additional principle of **Accountability** is added:
  - The controller shall be responsible for, and be able to demonstrate compliance with the principles

Legal basis for Processing

- We must understand all the information we process & document the legal basis for processing it
  - If someone asks, we need to be able to tell them what information we hold about them & why
- This must be made available on request to the ICO
- Most efficient way is to identify and audit all of our Information Assets
  - Document all of the Information we hold,
  - Identify where it came from and who we share it with.
  - Implement processes to ensure this is managed formally

Conditions for Consent

- Consent forms need to be more specific about nature of the use of the information
- Organisations must be able to demonstrate that consent was given
- Consent must be:
  - Freely given
  - Specific
  - Informed & unambiguous
- Consent can be withdrawn
- Parent or guardian must consent for child if under 13

Sensitive data

- Additional items in around Genetic, Biometric & health data
- DPA18 uses different terminology than GDPR which refers to Special Categories of data
  - Racial or ethnic origin
  - Political opinions
  - Religious or philosophical beliefs
  - Trade union membership
  - **Genetic data for the purpose of uniquely identifying a natural person**
  - **Biometric data for the purpose of uniquely identifying a natural person**
  - **Health data**
  - Data concerning a natural person's sex life or sexual orientation

- Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing
- This data cannot be processed unless specific conditions exist
  - For example, consent, legitimate interest, legal purposes.

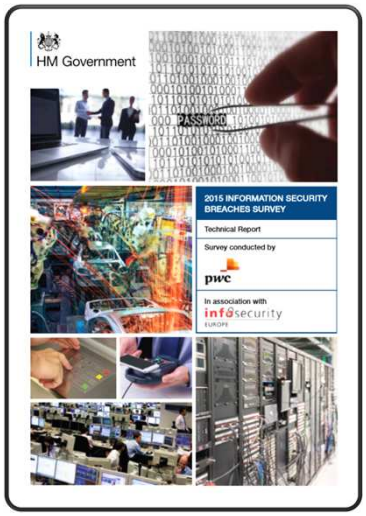
Rights of the Data Subject

- Applies to Articles 15 to 20
  - Article 15 – Right of Access
  - Article 16 – Right to Rectification
  - Article 17 – Right to Erasure
  - Article 18 – Right to Data Portability – common format, machine readable.
  - Article 19 – Right to object (to marketing, profiling, research)
    - Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
    - Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
  - Article 20 – Right to object to automated individual decision making

Breach notification

- Mandatory Breach notification for all organisations
  - Previously only mandatory for Health & social care
- Must report to ICO (Supervisory authority):
  - Nature of incident, categories and numbers of records
  - Name and contact details of a contact point
  - A description of the likely consequences of the personal data breach;
  - Measures taken / proposed to be taken
  - Mitigation applied to reduce adverse effects
- Report to individuals
- Processor to report to Controller
  - When breach is identified

Within **72** Hours



Independent Supervisory Authority for UK

- Independent, transparent appointment
- Tasks: monitoring, enforcement, awareness, complaints, investigations
- Powers: warnings, reprimands, orders, authorization
- Fines will be "effective, proportionate and dissuasive"
  - Nature of the breach, number of data subjects, level of damage
  - Intention/negligence, mitigating actions
  - Co-operation, self notified
  - Categories of data
  - Previous infringements

ico. Information Commissioner's Office

£9m eg: Security, Retention

£18m eg: Principles, Consent, Rights

DP Impact Assessments

- Mandatory where:
  - processing likely to result in high risk for rights and freedoms of individuals
  - new technologies are being implemented
- Must consult DPO (mandatory role)
- ICO expected to list where DPIA and/or authorisation required
- High risk – consult the ICO before processing
- Breach if no DPIA is carried out where required

Data Protection by Design | **Data Protection by Default** | **Data Minimisation**

Supply Chain Contracts

- Contracts must set out:
  - the subject matter and duration of the processing;
  - the nature and purpose of the processing;
  - the type of personal data and categories of data subject; and
  - the obligations and rights of the controller.
- Contracts must also include as a minimum the following terms, requiring the processor to:
  - only act on the written instructions of the controller;
  - ensure that people processing the data are subject to a duty of confidence;
  - take appropriate measures to ensure the security of processing;
  - only engage sub-processors with the prior consent of the controller and under a written contract;
  - assist the controller in providing subject access and allowing data subjects to exercise their rights
  - assist the controller in meeting its GDPR obligations
  - To delete or return all personal data to the controller as requested at the end of the contract; and
  - submit to audits and inspections

Data Protection Officer

- Data Protection Officer mandatory for public authorities & processors of large volumes of personal data
  - FoI definition used for public bodies
  - Government departments, legislative bodies, and the armed forces, Local government, NHS, Maintained schools and further and higher education institutions, Police
  - Public owned companies – wholly owned by the public sector
- Tasks include
  - Inform and advise
  - Monitor compliance
  - Awareness/training
  - DP Impact Assessments
  - Contact Point for ICO
  - Report directly to highest management
  - No conflicts of interests

Remedies in the court

- Compliance orders
  - A court could order data to be secured or order an organisation to refrain from taking certain actions that put compliance at risk
- Compensation for contravention of the DPA
  - Right to compensation "damage" includes financial loss, distress and other adverse effects.
  - The current act only allows for compensation if material loss occurred
- This will lead to a new industry in obtaining compensations for breaches
  - Including holding information that shouldn't be held
- The cost of compensation could outweigh any fine
  - Fines are dependant upon the management of a breach
  - Compensation will not be

Privacy Notices

- What information must be supplied?
  - Identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer
  - Purpose of the processing and the legal basis for the processing
  - The legitimate interests of the controller or third party, where applicable
  - **Categories of personal data**
  - Any recipient or categories of recipients of the personal data
  - Details of transfers to third country and safeguards
  - Retention period or criteria used to determine the retention period
  - The existence of each of data subject's rights
  - The right to withdraw consent at any time, where relevant
  - The right to lodge a complaint with a supervisory authority
  - **The source the personal data originates from and whether it came from publicly accessible sources**
  - Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
  - The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.
    - **Items in red not needed for Data obtained directly from data subject**

DPA / GDPR Myths

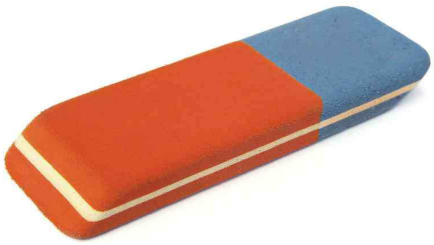
- GDPR won't be implemented due to Brexit
- The changes only affect either the public sector or the private sector
- The act provides prescriptive details on how to comply
- White papers about GDPR are written by experts
- You will need consultancy in order to become compliant
- If you buy certain products, you will be compliant
- You will need to change all your ICT to be compliant
- It will be expensive to comply with

Will GDPR affect you?

- Do you use your personal email account for Council business?
- Do you for example use your personal email account to print documents?
- If the answer to either of the above is YES GDPR could affect you.

What do you need to do?

- Do not use your personal email account for Council Business because you open it up to potential scrutiny for the purposes of SARs
- If you have to; delete all Council documents as soon as they are printed/received.



What do you need to do?

- If you suspect a data breach - regardless of how it occurred - if rights and freedoms affected
- 72 hours to report it

May 2018!