Get to Grips With Data Protection

Gill Smith
DP Assist
Data Protection Act - What’s It All About?

- Safeguard rights and freedoms of individuals
- 8 legally enforceable principles
- Enforced by the Information Commissioner - Christopher Graham
What do these have in common?
New EU Data Protection Regulations

- Individual’s rights strengthened - Right to be forgotten/erasure
- No charge for access to your own information or notification (registration)
- More reliance on consent and justification for collecting, using, disclosing information
- Notify breaches of principle – mandatory
- Privacy by design – built into systems
- Enforcement action against service providers (data processors)
Enforcement

Offences

- Unauthorised obtaining or disclosure of personal data (Section 55)
- Procurement – to acquire, sell or offer to sell information unlawfully
- Non-compliance - Enforcement or Information Notice
- Non-Notification and failure to notify changes to your Register Entry
- Forcing someone to make a subject access request to check their criminal past (Section 56)
- Public authority: when providing subject access request information, if you alter, deface, block, erase, destroy or conceal any information that the requester is entitled to.

Penalties

- Serious breach of principle – monetary penalty up to £500,000
- Offences – Now unlimited fine if Magistrates’ Courts
Which Hat Are You Wearing?

- For the Council e.g. serving on a committee?
- For your constituents?
- For your political party?
- Personal, domestic, recreational purposes?
Whose Information is Covered?

- Living identifiable individuals (of any age)
- Not de-personalised or statistical information
- Not businesses or organisations
- Not the deceased
Personal Data

- Makes a person identifiable from information that you have or could obtain about them
- Relates to them - helps you to learn, record, or decide something about them
- They are the focus
- Should be of biographical significance

Sensitive Personal Data

- Racial or ethnic origin
- Political opinions
- Religious or other beliefs
- Trade Union membership
- Physical or mental health or condition
- Commission or alleged commission of an offence
- Any offence proceedings their disposal or sentence of any court.
More Definitions

- **Data Subject** – person who the information is about
- **Processing** – obtaining, using, storing, destroying etc
- **Data Controller** - controls manner and purpose(s) of processing
- **Data Processor** - processes on behalf of data controller
- **Third Party** - Anyone except data subjects, employees, or agents of data controller
Principle 1 – Fair Processing

Provide a Privacy Policy, Privacy Statement or Fair Processing Notice:

- Data subjects should be informed of:
  - Identity of who they provide it to or nominated representative if you are not based in the UK
  - Purpose(s)
  - Anything else to make it fair. For example who you share information with

- Exemptions may apply:
  - Crime prevention/detection/apprehension
  - Taxation
  - Required by law to disclose
  - Disproportionate effort if you receive it from a third party
GET ALL THE INFORMATION YOU CAN, WE'LL THINK OF A USE FOR IT LATER.
**Principle 1 - Lawfulness**

- Must not contravene other laws such as:
  - Human Rights Act – Article 8
    - Right to respect for private and family life.
    (Privacy Impact Assessments)
  - Common Law Duty of Confidentiality
    Overrides:
    - Consent
    - Legal requirement or obligation
    - Crime prevention/apprehension or prosecution of offenders
    - Risk of harm to person or someone else
    - Public interest

Must Satisfy at least one Schedule 2 Conditions for Processing AND Schedule 3 (if Sensitive Data)
Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

- Applies to sending advertising materials (including newsletters, event information etc) – by text, email, fax.

- Includes unsolicited (including automated) phone calls to business and private individuals – check the Preference Service at www.tpsonline.org.uk

- Use of Internet Cookies on websites - small file of letters and numbers downloaded on to a device when websites accessed.

- Consent required

- Enforced by the Information Commissioner
Principle 2 – Secondary Use and Notification

Must not be used in any way that is incompatible (or clashes with) its ORIGINAL purpose

Assess:-
- Change of use? Seek consent?
- Disclosures to third parties?

Example - Social Media Use: Create a specific Councillor account or page to keep personal and political use separate. You can then share information with constituents and colleagues without disclosing personal information about yourself, friends and family.
Notification

Public register at www.ico.gov.uk

- £35 fee – annual renewal
- **Must** be kept accurate and up to date
- You must amend it within 28 days of changes such as new purpose(s)
- Criminal offence **not** to be registered or updated.

**Exemptions include:**

- Core business purposes
- No information held on computer

**Purposes, Types of people whose information is held, Types of information, Who it’s disclosed to, Overseas transfers Public Authority Security Info (not made public)**
Principle 3, 4 and 5 – Good Information Management

- Adequate relevant and not excessive
- Accurate and kept up to date
- Not held longer than necessary

Review, Retain, Destroy or Archive
Principle 6 Individual’s Rights

Subject Access

- What are individuals entitled to?
- What makes a valid request?

What Are Your Responsibilities When Responding To and Dealing With a Request?

- Optional:
Principle 6 Individual’s Rights

Subject Access

- To be informed if personal data held, and receive a description or copy of it **plus** purposes, sources and recipients (if available)

- Valid request – in writing, description of information sought, and fee (if charged), identity checked.

**Your responsibilities:**
- Confirm (or deny) information is held
- Provide it within 40 calendar days
- Check identity
- Make it intelligible
- Consider whether to withhold or provide 3rd party information
- Consider if exemptions apply (repeated requests, supply involves disproportionate effort, crime prevention/detection, references, legal professional privilege, management forecasting, negotiations etc)

**Optional:** Charge a fee - Standard Fee = £10 (optional)
Principle 6 Individual’s Rights

- Have personal data corrected or deleted if inaccurate or misleading (via courts)
- Prevent processing likely to cause damage or distress
- Object to direct marketing

- Object to automated decision making
- Compensation
- Request an assessment
Man's £18k payout after ex-girlfriend viewed his medical records
Principle 7 - Take Appropriate Security Measures
Principle 7 What is “Appropriate?”

Conduct A Security Risk Assessment:

- Whose information is it?
- What personal data are held, how and where?
- Vulnerabilities and threats?
- Nature of harm/distress caused to them if unauthorised or unlawful access/loss/damage/theft/disclosure
- Consequences to your organisation?
- What technology is available and at what cost?
Sam Green
Days Absent: from work: 7
Reason Flu
GP: Dr Hodder
Principle 7 - Take Appropriate Security Measures

- Must ensure: Confidentiality, Integrity, Availability
- Control Access: Secure passwords (change default ones), safe storage and transit, protect from others, secure destruction
- Protect Your Information Systems
  - Secure, long, difficult to guess passwords, changed regularly
  - Anti-Virus, malicious software and hacking protection
  - Secure networks (including WIFI - Wireless)
  - Removable Media - Encryption eg memory sticks
  - Keep software upgrades up to date
Using Your Own Device

- **What work information is stored on it?** – Keep it separate from private use
- **Where is it stored?** (memory card, cloud) – Keep it secure (encryption, trusted providers)
- **What apps are installed or downloaded?** Obtain from trusted providers
- **Who has access to it?** – Keep it away from others
- **How is it secured?** Strong password, locks if not used, pin number, encrypted, up to date anti-virus protection, latest security upgrades installed?
- **What is it connected to?** Beware public networks – do not automatically connect.
- **What happens if it is lost or stolen?** Can it be wiped securely?
Principle 7 - Take Appropriate Security Measures

- Protect from fire, flood, and accidental damage - Safes and off-site storage of backups (test them), disaster recovery plans
- Organisational measures - ensure employee reliability
  - Policies, procedures, training, vetting, keep informed
  - “Data Protection and Information Security Key Points for Councillors”
  - “ICT Guidelines for SSDC Councillors”

- Service Providers (Data Processors)
  - Must have written contracts
  - Act only under your instructions
  - Ask for security guarantees and action to be taken
  - Right of audit/inspection/compliance monitoring
Principle 8 - Overseas Transfers

OK to send information overseas if:

- Country or territory is within the European Economic Area
- Or adequate protections in place
  - ”Safe” or Third Countries eg Canada
  - Safe Harbor – USA companies or organisations

If not, then

- Must satisfy Schedule 4 Conditions eg seek consent, can transfer if to protect vital interests, public register, contract in place etc

BEWARE - includes internet and social media use
Dealing with Disclosures

- Was individual informed about it? Reasonable expectation?
- Lawful? Condition for processing satisfied? Duty of confidentiality?
- Is disclosure required by law? (Section 35) eg Member powers to inspect documents necessary for your work
- In connection with legal proceedings, seeking legal advice or establishing, exercising or defending legal rights? (Section 35)
- For prevention and detection of crime or taxation? Overriding public interest? (Section 29)
- Emergency? Matter of life or death?
- Freedom of Information or Environmental Information request?
And finally, don’t let this happen to you......