Preparing for the new General Data Protection Regulation

Maureen H Falconer
Regional Manager – Scotland
Information Commissioner’s Office
GDPR Session Overview

- Legislative landscape
- Definitions
- Rights for individuals – SAR changes
- The Principles
- The ‘new’ Accountability principle
- Advice and Guidance
Legislative landscape

From DPA 1998 to:

GDPR 2016

LED 2016

and, eventually,

DPA 2018

The DP Bill is currently going through the UK Parliament and is hoped to receive Royal Assent by April.
The DP Bill

**Part 1** Overview & definitions.

**Part 2** General data processing in line with GDPR & outside the scope of EU law (applied GDPR).

**Part 3** LED provisions.

**Part 4** National security.

**Part 5** Functions and duties of ICO.

**Part 6** Enforcement & ICO’s powers.

**Part 7** Miscellaneous provisions: regulations, penalties and territorial application.

+ **18 Schedules**
Key Definitions
What is data?

Recorded on computing equipment

Recorded on certain manual records
What is processing?

From obtaining it, through to...

...putting it beyond use.
Who is responsible?

Data controllers

Data processors

Contract
What is *Personal* data?

Any information relating to an identified or identifiable [living] natural person who can be identified, directly or indirectly, in particular by reference to an identifier.
Special categories

- Race or ethnicity
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health
- Genetic or biometric
- Sexual life or orientation
- Criminal offences
Individuals’ rights and organisations’ obligations
Individuals' rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to stop direct marketing
- The right to object
- Rights related to automated decision-making and profiling
It’s a Principled based approach
Six GDPR Principles

Personal data should be:
(a) processed lawfully, fairly and in a transparent manner,
<table>
<thead>
<tr>
<th>What information must be supplied?</th>
<th>Obtained from individual</th>
<th>Not obtained from individual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity and contact details of the controller and where applicable, the controller’s representative) and the data protection officer</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Purpose of the processing and the lawful basis for the processing</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>The legitimate interests of the controller or third party, where applicable</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Categories of personal data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any recipient or categories of recipients of the personal data</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Details of transfers to third country and safeguards</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Retention period or criteria used to determine the retention period</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>What information must be supplied?</td>
<td>Obtained from individual</td>
<td>Not obtained from individual</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>The existence of each of data subject’s rights</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>The right to withdraw consent at any time, where relevant</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>The right to lodge a complaint with a supervisory authority</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>The source the personal data originates from and whether it came from publicly accessible sources</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>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</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Conditions for processing

Personal data
- Consent
- Contract with the individual
- Comply with a legal obligation
- Protecting vital interests
- Public function in the public interest
- Exercise of official authority
- (Legitimate interests of the data controller, but not prejudicial to the person)

Special Category data
- Explicit consent
- Employment, social security, social protection law
- Vital interests
- Not for profit religious, political or trade union bodies
- Put in public domain by the person
- Legal proceedings/advice
- Substantial public interest based on law
- Health, medical, social care
- Public health
- Archiving, research, statistical purposes

Additional conditions likely to be in the new UK DP Bill
What’s not consent?

✖ Relying on silence, pre-ticked boxes or inactivity;

✖ Having no genuine or free choice or being unable to refuse or withdraw without detriment;

✖ In any specific case, having an imbalance between the person and the controller, especially where the controller is a public authority and it’s unlikely for consent to have been freely given in all the circumstances of that case;

✖ Not allowing separate consent to be given to different processing despite it being appropriate in any individual case; or

✖ Making the performance of a contract dependent on consent when it’s not necessary for such performance.
International transfers

A Layered Approach:

**Art 45**
- Does the third country provide an adequate level of protection?
- e.g. DPA or equivalent law safeguarding personal data

**Art 46**
- If not, can the data controller provide adequate safeguards?
- e.g. model contract clauses, binding corporate rules, anonymisation, encryption, etc.

**Art 49**
- If not, would derogations apply?
- e.g. explicit consent, contract, public interest, legal claims, vital interests, compelling legitimate interest.
Six GDPR Principles

Personal data should be:
(a) processed lawfully, fairly and in a transparent manner,
Accountability
The Accountability Principle

The controller shall be responsible for, and be able to demonstrate compliance.
Data Protection Impact Assessments
Record of processing activities

• DC name and contact an DPO
• Purposes of processing
• Categories of data subjects and personal data
• Categories of recipients
• Transfers to third countries or international organisations
• Retention and destruction timeframe
• Security measures for safekeeping

_Article 30 GDPR_
Data security breach notification
Data Protection Officer
Feeling in need of a lifeline??
Preparation for the General Data Protection Regulation (GDPR) 12 steps to take now

1. Awareness
   You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2. Information you hold
   You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3. Communicating privacy information
   You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4. Individuals' rights
   You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5. Subject access requests
   You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6. Lawful basis for processing personal data
   You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7. Consent
   You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8. Children
   You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9. Data breaches
   You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10. Data Protection by Design and Data Protection Impact Assessments
    You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11. Data Protection Officers
    You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12. International
    If your organisation operates in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.
GDPR resources

https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/
Guide to GDPR

Self assessment toolkit

Keep in touch

ICO Scotland
45 Melville Street
Edinburgh EH3 7HL
T: 0303 123 1115 E: Scotland@ico.org.uk

Subscribe to our e-newsletter at www.ico.org.uk
or find us on...

@iconews