UNIVERSITY OF Southampton

EU General Data Protection Regulation: 'GDPR'

Coming into force on 25 May 2018

What you need to know *now*: 'why comply?', 'what's new?', and 'how can we comply?'

Alison Knight, Legal Services & Data Governance

Background

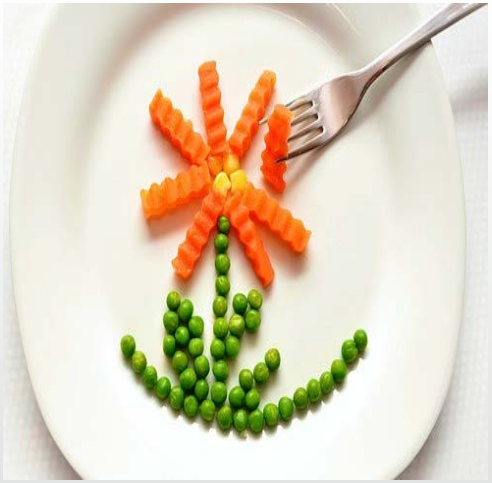
- GDPR aims to strengthen data protection laws to make them fit for the digital age by giving people more control over their own data
- The current UK Data Protection Act 1998 was derived from EU law (the Data Protection Directive) which is being replaced by the GDPR
- The text of GDPR will apply throughout EU Member States, directly embedded into new national data protection legislation (incl. a new UK Data Protection Act 2018 to come)
- Brexit does not affect the implementation of GDPR

‘Why?’ (i) – A ‘sharpened carrot’ approach

"If your organisation can't demonstrate that good data protection is a cornerstone of your business policy and practices, you're leaving your organisation open to enforcement action that can damage both public reputation and bank balance.

But there's a carrot here as well as a stick: get data protection right, and you can see a real business benefit.”

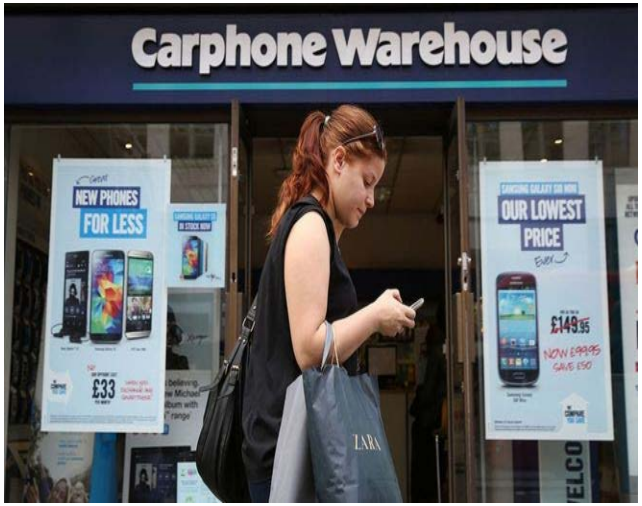
Elizabeth Denham, The UK Information Commissioner



"A company as large, well-resourced, and established as Carphone Warehouse, should have been actively assessing its data security systems, and ensuring systems were robust and not vulnerable to such attacks…

Carphone Warehouse should be at the top of its game when it comes to cyber-security, and it is concerning that the systemic failures we found related to rudimentary, commonplace measures."

Elizabeth Denham, The UK Information Commissioner



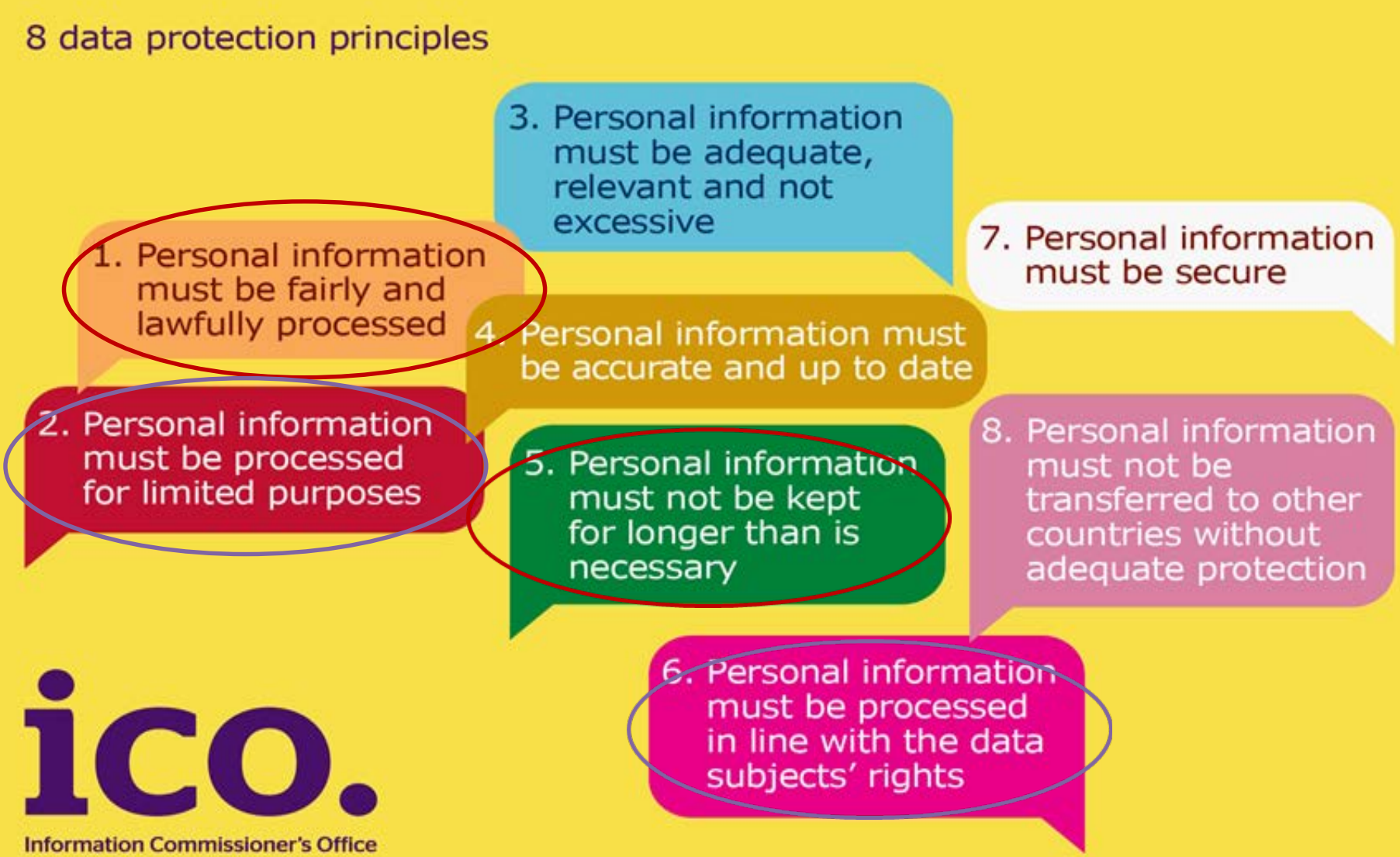
‘Why?’ (ii) – New fine levels

Major breaches of data protection are subject to administrative fines: whichever is higher of the following:

- **up to 20,000,000 EUR, OR**
- **up to 4 % of the total worldwide annual turnover of the preceding financial year (in the case of an undertaking)**
- **Focused on incidents which are likely to cause damage and distress**

Medium breaches of data protection are subject to administrative fines: whichever is higher of the following:

- **up to 10,000,000 EUR, OR**
- **up to 2 % of the total worldwide annual turnover of the preceding financial year (in the case of an undertaking)**
- **Focused on process failures. For example, failure to report ‘High risk’ breaches to the ICO and the relevant data subjects within 72 hours.**



The main data protection principles –

Key message: Establishing data processing purpose is fundamental to GDPR compliance

‘What’s New?’ - Demonstrating compliance

Principle of Accountability: “*The **controller*** [who controls the means / purposes for which personal data are processed] *shall be responsible for, and be able to demonstrate compliance with the Principles”*

New requirements:

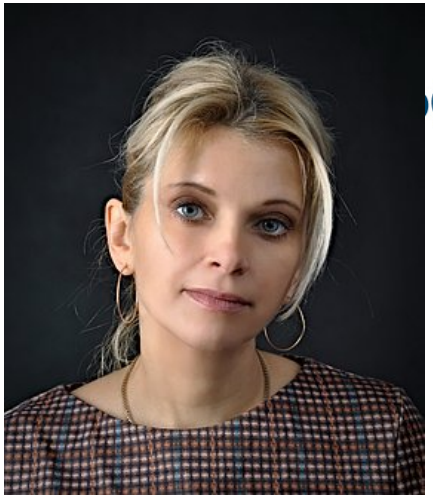
- Maintaining records on processing activities
- A **risk-based approach** when it comes to personal data management: implementing *appropriate* **technical** and **organisational** measures to comply with GDPR principles
- Data protection ‘**by Design’** and ‘**by Default’**
- Data protection impact assessments
- Appointment of a data protection officer
- Direct liability for data **‘processors’**

Any information relating to an identified or identifiable natural person

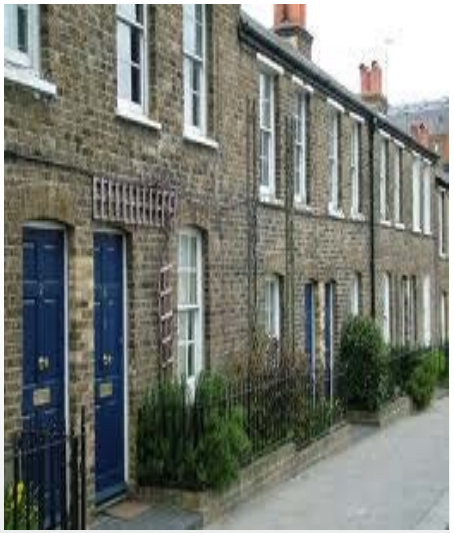
An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to:

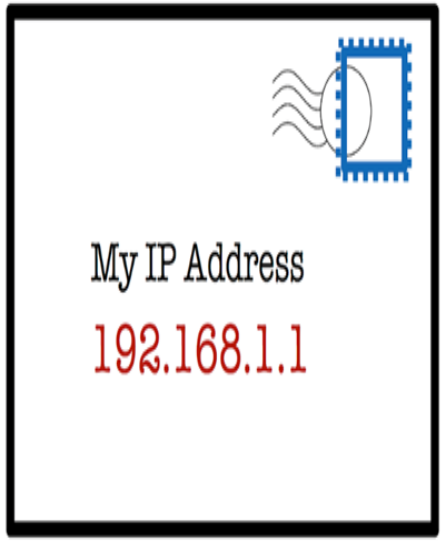
- an identifier such as a name, an identification number, location data, an online identifier or
- to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”

Compare the concept of ‘sensitive’ personal data – delimited categories



	A
1	**Full Name List**
2	Heidi Kim Lee
3	Mary Elizabeth Smith
4	William Jefferson Clinton
5	George Walker Bush
6	Tyler Matthew Smith
7	Ryan Matthew Keagy
8	Sammy C. Watson
9	Charles Henry Pearson
10	Suhaana Hyatt Khan





Personal data – wide definition but ultimately context focused

‘How?’ (i) – what is the University doing?

- GDPR Working Group
- Information *Personal Data* Asset Register being compiled
- Review of agreements with other organisations that share personal data with the University (in particular, flows of personal data into / out of the EEA)
- Review of the University's privacy policy, and consent form / privacy notice templates
- Compiling retention protocol / schedules
- Where necessary, carrying out in-depth ‘data protection impact assessments’

‘How?’ (ii) – What can you do?

Compliance duty	Activities
Roles & responsibilities	• **READ AND CIRCULATE OUR ‘DO’S AND DON’TS’** • Appointment of local data protection champions • Add data protection compliance issues to the agenda of all high level meetings concerning operations
Auditing	• Local auditing of personal data processing activities and data flows to align with university policies. • Findings should be recorded and periodically reviewed
Incident management	• Implementation of a robust policy and process to manage security incidents
Training & Awareness	• E-training being rolled out for all staff and the possibility for bespoke training • Consider the arrangement of data protection ‘clinics’ for staff to discuss their personal data processing concerns

Where can you get help?

Guidance type	Web link
Sharepoint	• https://intranet.soton.ac.uk/sites/gdpr/Pages/Home.aspx • These slides and the accompanying packs to circulate are also to be uploaded to Sharepoint
Email us	• **General enquiries:** gdpr@soton.ac.uk • **Legal**: gdprlegal@soton.ac.uk • **Data Protection:** dp@soton.ac.uk • **Information Security:** infosec@soton.ac.uk • **Chief Information Office**: sjc@soton.ac.uk
ICO Guide to the GDPR	• https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
ICO 12 steps to preparing for the GDPR	• https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

UNIVERSITY OF Southampton

Questions/Discussion Time