Welcome

- Chair's address – Barry Warne, hlw Keeble Hawson
- GDPR Seminar- Sarah Power, hlw Keeble Hawson
- Cybersecurity and GDPR – Dominic Ryles, Exertis UK

GDPR: the steps you have to take, and how to take them in time

Sarah Power

sarahpower@hlwkeeblehawson.co.uk

Seminar Outline

- Basics
- Steps to success
- How to get “wrong” right

Before you ask…

- 25 May 2018
- Brexit won’t affect the new rules
- Yes, GDPR affects you!

Getting started

- You are probably part-way there already
- Know your operations
- Be aware of the risks and the benefits of getting GDPR right

Personal Data

- Identifies
- A living person
- Directly or indirectly

Sensitive Personal Data

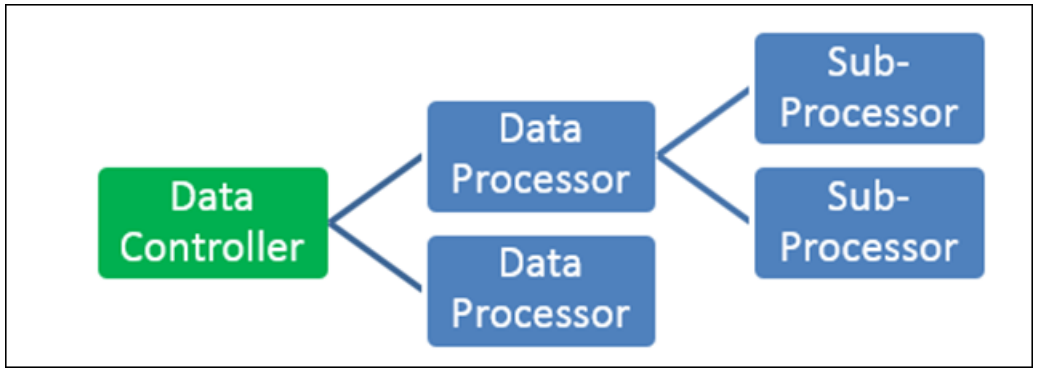
- Health
- Sexual orientation
- Political opinion
- Religion
- Race
- Genetic or biometric data

Personal data is a valuable asset

- “Free Wi-Fi, great!”
- “Shall we just get an Uber?”
- “I’ll just order it online”
- iPhone Touch ID is enabled

What's in a name?

- Data Controllers
  - What
  - How
  - Why



- Data Processors
  - Prescribed processing, on behalf of a data controller

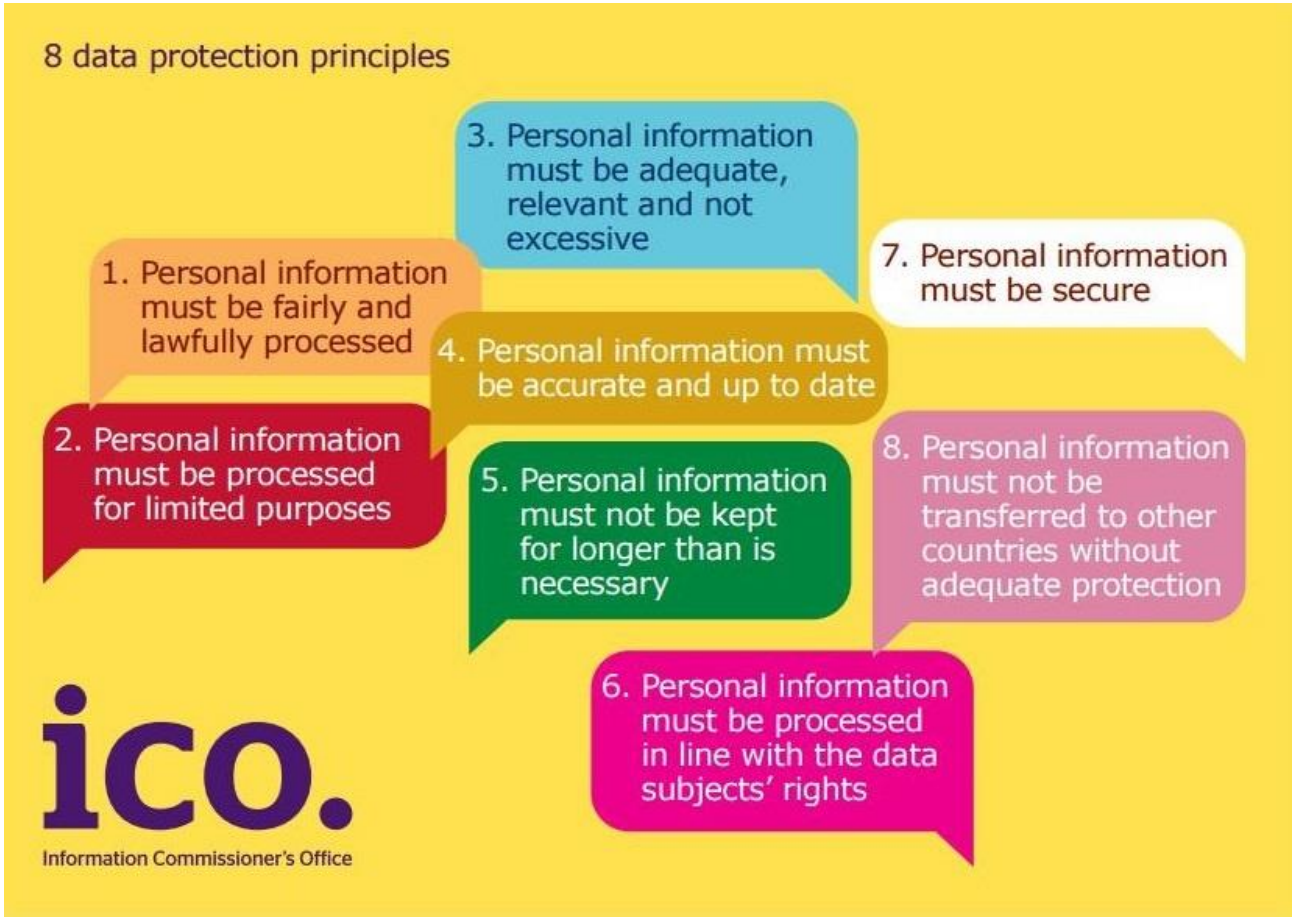
- BOTH can be held liable for data breaches

Your GDPR mantra

Data rights

- Right to be informed
- Right of access
- Right to rectification
- Right to restrict
- Right to “be forgotten”
- Right to data portability
- Right to object
- Rights in relation to profiling and automated decisions

Principles of Data Protection



Plan to succeed

1. Identify data and processes
2. Establish and record your lawful basis
3. Communicate privacy information
4. Update policies and procedures
5. Staff training
6. Review data-sharing agreements
7. Risk assess (DPIAs)
8. Choose a DPO

Step 1: Take a bird's eye view

Data Mapping

- What have we got?
- Where did it come from?
- What do we do with it?

Step 2: Own it

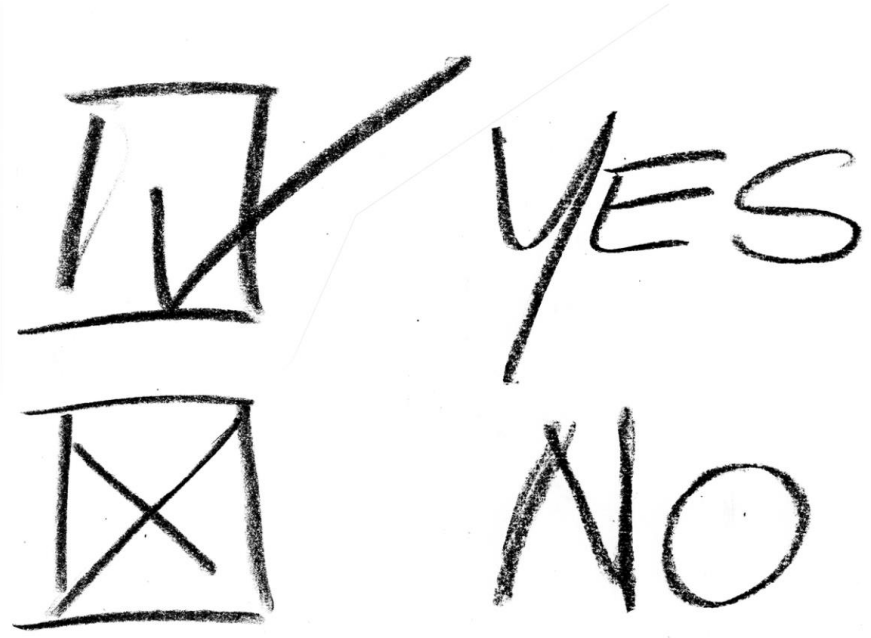
Recording your Lawful Basis for processing

- You should be able to justify your decisions to process certain data in a particular way in for a particular purpose
- You need to be able to point to at least one Lawful Basis;
- Processing sensitive personal data needs one PLUS an additional reason

Lawful Basis

Consent – but not as you know it

- Informed
- Freely given
- Positive



“We’ve already got consent”

- Will it stand up after 25 May 2018?
- Refresh?
- Marketing materials and the “soft opt-in”

Did you hear about Honda?

Consent – is it your best option?

- Sometimes need it
- Can you use another basis?
- Avoid over-reliance

Contract

- Performance of a contract
- Pre-contract enquiries
- Is it necessary?

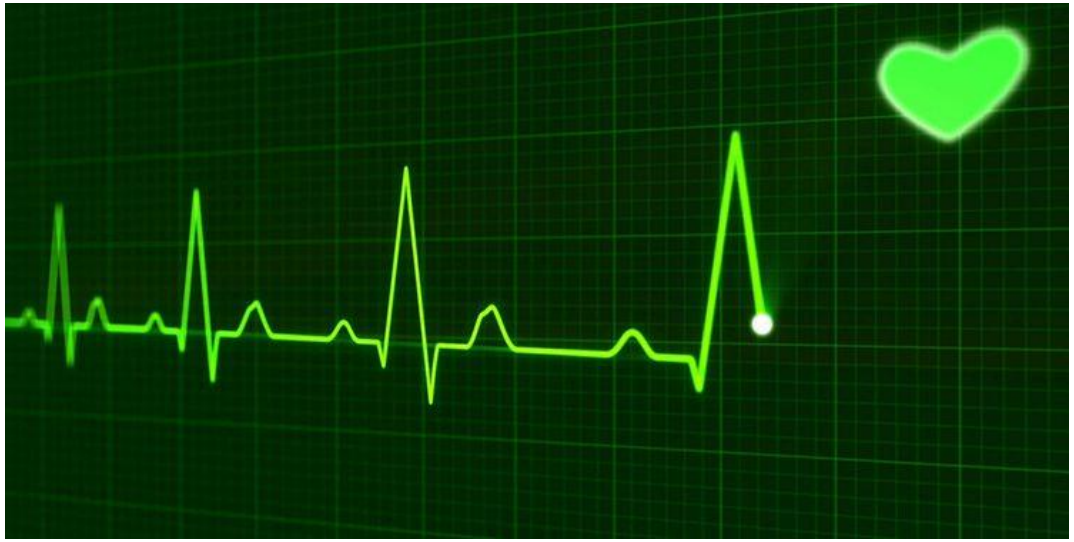
Legal Obligation

- What obligation are you complying with?
- Is it necessary?
- E.g. disclosing salary details to HMRC

Vital Interest

- Life or death

- Incapable of giving or withholding consent



Public Task

- Performance of a public function
- Public authorities
- Power conferred by law

Legitimate interests

- Ordinary honest business practices
- Balancing act
- Flexible, but not a catch-all

Step 3: Communicate your policy

- Privacy notices ensure data subjects are informed
- Ensure data controllers act transparently and can be accountable
- Must be clear and appropriate for its audience

Step 4: Review policies

- “We’ve always done it this way”
- Document decisions and procedures
- Communicate them to staff

Step 5: Spread the word

- All staff need to be aware of relevant policies
- Before they come into contact with personal data
- Record training practices

Did you hear about the NHS?

Step 6: Review data-sharing agreements

- Prescribed clauses
- Must be in writing
- Describe the extent of the data shared and processing to be carried out

Step 7: Do I need a Data Impact Assessment?

- Risk assessments for certain types of processing
- Identifies risks, and what strategies are going to help reduce those risks
- Must be used where there is a new technology being used, or where there is a high risk to the rights of the data subject

Step 8: Choose a Data Protection Officer

- Few will be required to appoint one
- DPOs help to implement training, assist with audits, monitor compliance and liaise with regulators as necessary
- Must be facilitated
- Internal/external, but cannot have a conflict of interest

Data Breaches – are easier than you think

- Accidental or unlawful
- Destruction or loss
- Alteration
- unauthorised disclosure
- unauthorised access.

Weak links

- Technology / third parties – Cybersecurity and ransomware

  Did you hear the news about Uber?

- Prying staff

  Did you hear the news about the NHS?

  Did you hear about T-Mobile?

- Avoidable mistakes

  Did you hear the news about HMRC?

  Did you hear the news about Norfolk County Council?

  Did you hear about Brighton University Hospital?

Reporting Data Breaches

- Internal reporting and documenting of all breaches
- May have to inform the ICO (72 hours)
- May have to inform the data subject (as soon as possible)

All is not lost

- Heavy fines for serious breaches
  - €10m or 2% global turnover
  - €20m or 4% of global turnover
- ICO say will not fine to financially cripple
- Relevant factors:
  - Any mitigation
  - Extent of co-operation with the ICO
  - Pro-active notification of the breach

Subject Access Requests

- Must respond within 1 month of request
- Can agree an extension
- Free of charge (unless repetitive, or manifestly unfounded)

Security

- Pseudonymisation
- Encryption
- Storage and destruction

Marketing

- Privacy and Electronic Communications Regulations

- Email marketing – usually requires specific consent

- Soft opt-in for previous customers
  - Similar product or service
  - Continually given them the choice to opt out

Can’t write fast enough?

sarahpower@hlwkeeblehawson.co.uk