Overview

- **Introduction:**
  - Background
  - Current law
  - Reform agenda
  - PECR
  - Brexit

- **Focus:** changes under the GDPR

- **Finish:** how to comply
Fines

Current fines (Data Protection Act 1998) vs. Fines from 2018 (GDPR)

- £500,000
- €20,000,000
The year 1995

Welcome to Amazon.com Books!

One million titles, consistently low prices.

(If you explore just one thing, make it our personal notification service. We think it's very cool!)

Spotlight! -- August 16th

These are the books we love, offered at Amazon.com low prices. The spotlight moves EVERY day so please come often.

One Million Titles

Search Amazon.com's million title catalog by author, subject, title, keyword, and more... Or take a look at the books we recommend in over 20 categories... Check out our customer reviews and the award winners from the Hugo and Nebula to the Pulitzer and Nobel... and bestsellers are 30% off the publishers list...
Current law

- **Data Protection Directive (95/46/EC)**
  - Each state has own law
  - 20 years old
  - Fragmented

- **Data Protection Act 1998**
  - Implements 1995 Directive
  - Principles based
  - Data control
Reform

- Timeline
  - Jan 2012: proposed
  - Dec 2015: agreed
  - May 2016: transition period

- Directly applicable
- Evolution not revolution
- Principles based
- More teeth
- Accountability
PECR reforms

- Privacy and Electronic Communications Regulations 2003
  - Electronic communications
  - Web privacy/cookies
  - Unsolicited e-communications
- Rules-based
- Marketing
- Proposed reform
  - Align with GDPR
  - 25 May 2018
  - Not yet final
Brexit

44%
Brexit

- GDPR will enter into law
  Adequacy decision
- Uncertainties remain
  EU court judgments
  Role in EDPB
  Cross-border enforcement
  EU representatives
Key concepts

- Personal data
- Special categories of personal data
- Controller
- Processor
Important changes

- Principles/Accountability
- Lawful grounds
- Processor liability
- Consent
- Profiling
- Data protection impact assessments
- Data protection officers
- SARs
- Right to be forgotten
- Right to data portability
- Contracting
- International transfers
- Security
- Breach reporting
- Registration requirement
Principles

1. Fair and lawful
2. Purpose limitation
3. Storage limitation
4. Data minimisation
5. Accurate and up to date
6. Confidentiality/integrity (security)

Also, new accountability principle
From time to time, we may allow other similar or partner organisations to contact our supporters. If you do not wish to hear from them, tick here. □
Lawful grounds

- Consent, or necessary for:
- Contract (performance/request)
- Legal obligation
- Vital interests
- Public interest/official duty
- Legit interests of controller/3rd party unless overridden by interests/rights of DS or public authority
If you would like us to no longer continue to stop not sending you marketing emails on a weekly basis please indicate YES by not checking the box below.
Consent

freely given, specific, informed, unambiguous indication of wishes by statement or clear affirmative action

- NO implied consent, opt-outs, pre-ticked boxes
- Granular
- Unbundled
- Identify third parties
- Records
- Refresh (?)
Are your details correct?

- **Honda (£13,000)**
  
  289,790 emails

  Update preferences

- **Flybe (£70,000)**

  3.3m emails

  Update preferences

  Prize draw
Processor liability

- Instructions
- Security
- Notify breaches
- Written records
- Cooperate with controller and ICO
- Data protection officer
- No subcontracting (without consent)
Processor liability
Impact Assessments

- Already good practice
- GDPR requires for new high risk technology/process
- Stop and think
- Soon as possible
- Article 29 WP guidance
Data Protection Officers

- Public authority or
- Core activity is processing:
  - Requiring regular/systemic monitoring of data subjects
    - Sensitive PD on a large scale
- Data protection expert
- 3rd party contractor
- Independent
Subject Access

- 1 month
- No fee (usually)
- More information:
  - Storage period
  - Non-EEA transfers/safeguards
  - Data sources
  - Subject rights
- Derogations
Right to be forgotten
Right to be forgotten

- Erasure
- Without undue delay
- Grounds
  - PD not required
  - Consent withdrawn
  - Subject objects (and no overriding legit ground)
  - PD unlawfully processed
- Not absolute
Data Portability

- Applies to PD
  - Provided by subject (including by activity)
  - Processed automatically
  - Processed on consent/ performance of a contract
- Transmit to other controllers
- Technically feasible
- Structured, common e-format (e.g. CSV file)
- Overlap with other rights
Each of the parties shall comply with all applicable data protection law when processing personal data in connection with this Agreement.
Contracting

- Controller responsible for processors
- Written contract
- Requirements include:
  - Compliance with instructions
  - Assist with requests
  - Delete or return on termination
  - Compliance, audits, inspections
  - Security measures
- Standard contracts?
International transfers

- Currently
  - SCCs, BCRs
  - Privacy shield
  - Whitelist countries

- Largely the same, except
  - New SCCs?
  - Codes of Conduct
  - Certification Schemes
  - No controller adequacy decisions
“[Our data] wasn't encrypted, nor are you legally required to encrypt it. We have complied with all of our legal obligations in terms of storing of financial information.”

Dido Harding, CEO of TalkTalk

October 2015
Security

- “appropriate technical and organisational measures”
- Proportionality, risk based, consider
  - Pseudonymisation/encryption
  - Integrity/confidentiality/reliance of systems
  - Ability to restore availability/access
  - Security testing / evaluation processes
- Must
  - Demonstrate
  - Review/update
Breach reporting

- Currently ICO expects “serious” breaches notified
- GDPR
  - Processors report to controllers
  - Controllers report all breaches to ICO unless *unlikely to risk rights and freedoms of natural persons*
  - Controller report severe breaches to data subjects
- Report to ICO within 72 hours
Registration

- Currently data controllers register
- Criminal offence!
- GDPR to abolish
- New fee system?
- Higher fees?
8 simple rules

1. Be transparent
2. Know purpose
3. Know lawful ground
4. Stick to the *principles*
5. Understand subject’s rights and your responsibilities
6. Lead from the top
7. Use common sense
8. No exceptions, no excuses
“Your name will also go on the list. What is it?”

“Don’t tell him Pike”

Don’t panic!

Most data breaches are avoidable and result from a failure of common sense
Feeling overwhelmed?

- Wrong fax number
- Emails cc’d instead of bcc’d
- Unencrypted laptop stolen from car
- Unencrypted laptop stolen from office
- Filing cabinet auctioned, forgot to remove contents
- Moved offices, left video recordings
- Moved offices, left papers behind
- Unencrypted USB sticks lost
A few ways we can help

- Privacy policies and notices
- GDPR compliant policies/contracts
- SAR response templates
- Training and workshops
- Risk assessments
- Breach reporting advice
- Direct marketing advice
Further reading

- **Information Commissioner’s Office**
  - Preparing for the GDPR: 12 steps to take now
  - Consultation: GDPR consent guidance
  - Privacy notices, transparency and control
  - Direct Marketing Code of Practice
  - Conducting Privacy Impact Assessments: Code of Practice
  - Discussion paper on profiling

- **Article 29 Working Party**
  - (Draft) Guidance on DPOs
  - (Draft) Guidance on data portability
  - Guidance on data protection impact assessments