Future proofing the workforce

HR conference – 27 April 2015

Protecting confidential information in a mobile workforce

David Mears & Hannah Lyons

ncvo

RUSSELL-COOKE | SOLICITORS

Agenda

- Quiz!
- Brief overview of Data Protection law and confidentiality
- What can go wrong? Common mistakes and how to avoid them
- Key issues and developments relating to HR
- Questions and comments?

QUIZ

1. What is a person who collects data about people called?

a) Information Commissioner

b) Data User

c) Data Controller

2. Which of these is an example of sensitive personal data?

a) Age

b) Religion

c) Address

3. Is a photograph of a person personal data?

4. How many Data Protection Principles are there?

a) 12

b) 10

c) 8

5. How long can personal data be stored?

a) Only for as long as necessary

b) One year

c) There is no time limit

Brief Overview of Data Protection Law and Confidentiality

Data Protection

- Collection and use of personal data is governed by the Data Protection Act 1998 (DPA)
- DPA applies to the **processing** of personal data-

  ICO: *'It is difficult to think of anything an organisation might do with data that will not be processing'*
- 8 Data Protection Principles that must be complied with when processing personal data

DPA: Some definitions

- **'Data Subject' –** anyone whose Personal Data is processed.
  - Includes: individuals on contact lists, employees, clients etc.
- **'Data Controller' –** individual/organisation who decides how and for what purpose Personal Data is to be processed
  - Excludes employees
- **'Data Processor'** – individual/organisation who processes Personal Data on behalf of the Data Controller
  - Must act on instructions and have a written contract
- The Data Controller is responsible for complying with the DPA, even if 'processing' is outsourced to a Data Processor

Sensitive Personal Data

- DPA also applies to the processing of 'Sensitive Personal Data'
- Additional steps must be taken to protect it
- **'Sensitive Personal Data' –** information about the Data Subject's:
  - racial/ethnic origin
  - political opinions
  - religious/similar beliefs
  - trade union membership
  - physical/ mental health
  - sexual life
  - offences (commission of and proceedings)

Consent

- Can be verbal, but it is good practice to obtain written consent.
- Must be 'freely given, specific and informed'
- Consent to process 'Personal Data' - may be inferred from something the Data Subject does (e.g. giving information without being prompted) but not from what they fail to do
- 'Explicit consent' is required to process 'Sensitive Personal Data' – must be given in response to you explaining why the information is required and how it will be used

Exercise:

A charity is proposing to send a monthly newsletter to its members. The email it sends out says, "We will add you to our mailing list, unless you tell us otherwise." What is wrong with this? What should be included instead?

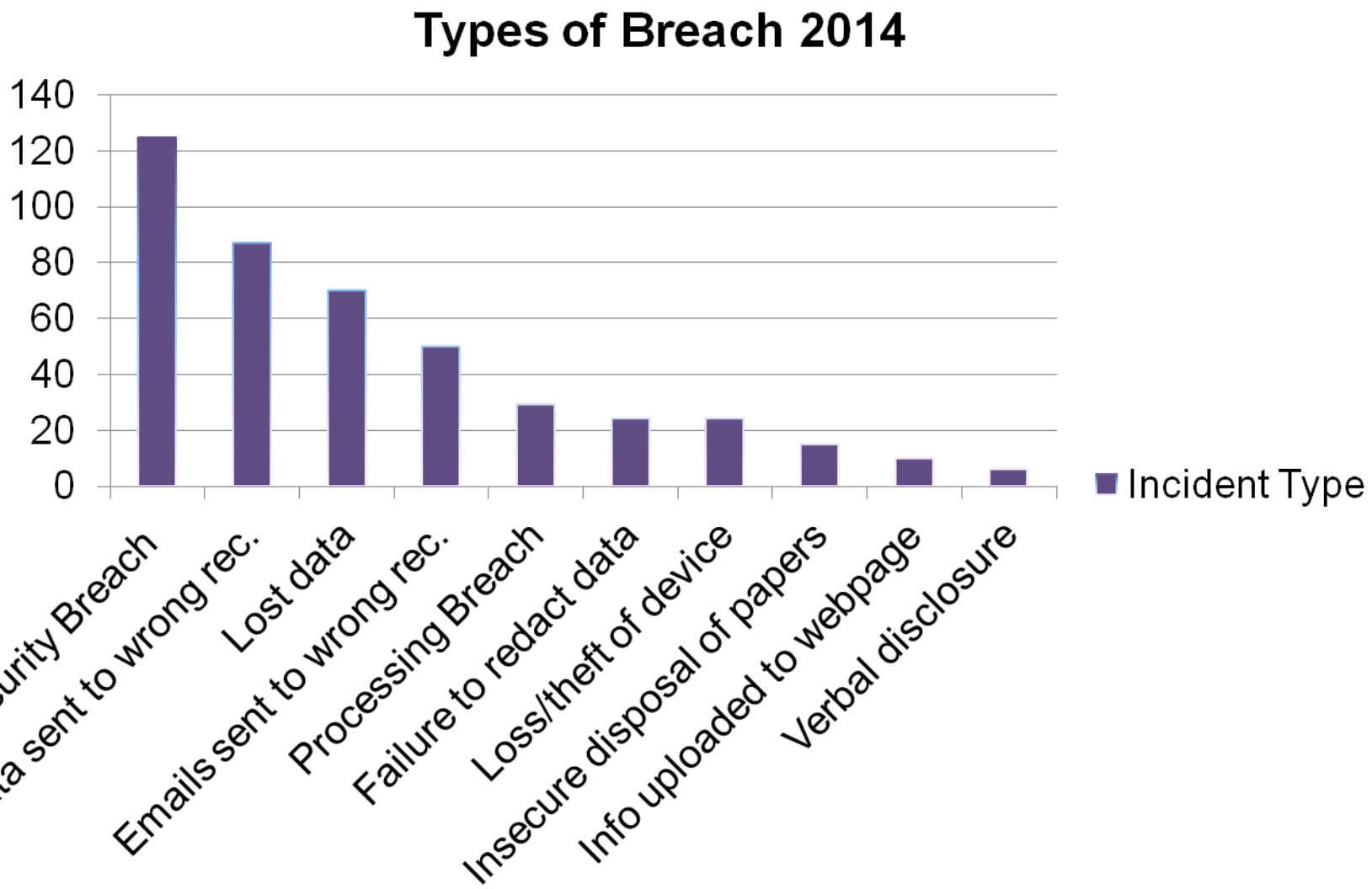
Confidentiality

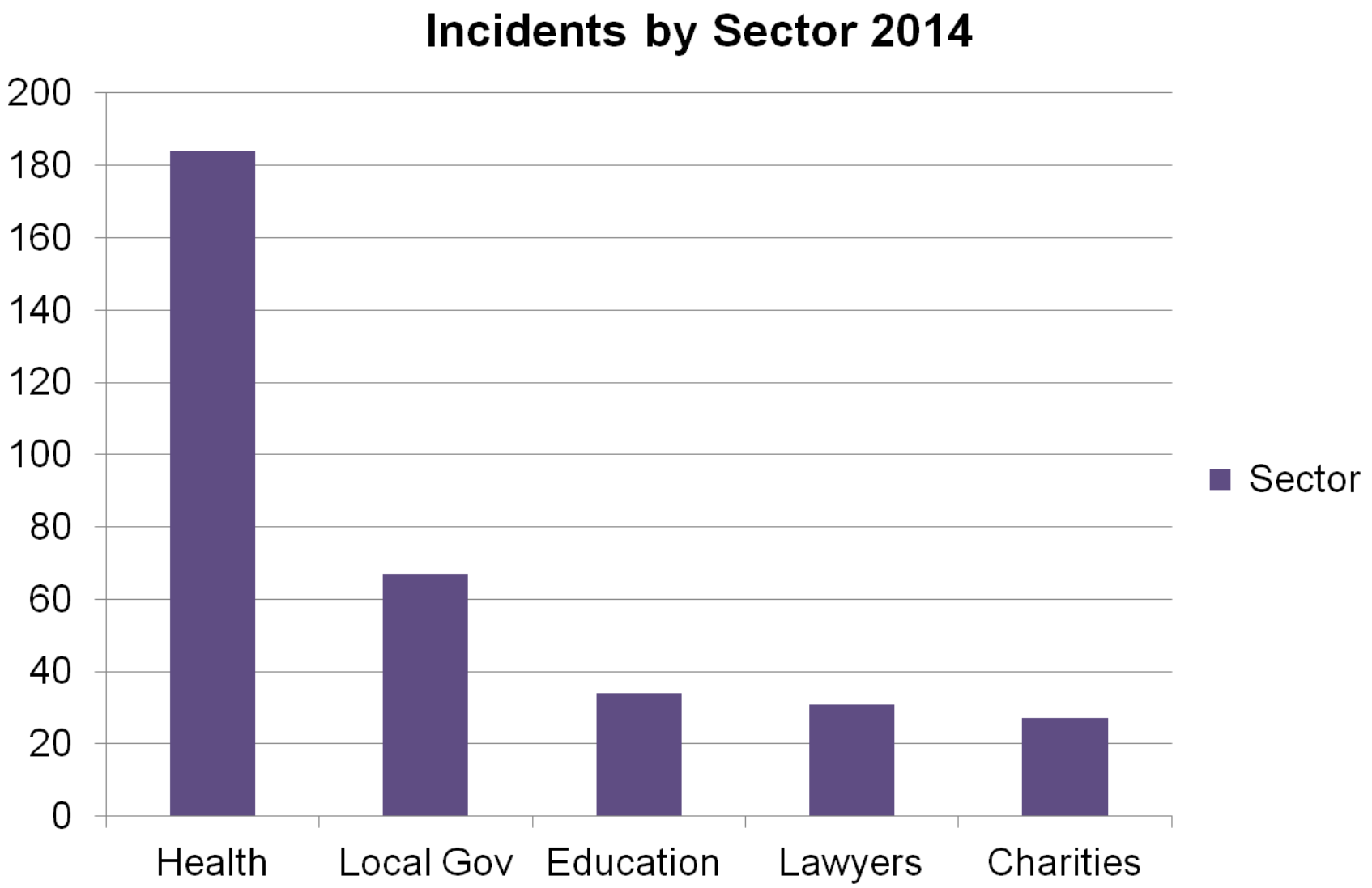
- Distinct from Data Protection
- Protects confidential information not protected by the DPA e.g. verbal communications, plans, proposals etc.
- Confidentiality may be imposed by contract, arise due to the nature of the relationship (solicitor and client) or may be implied because of the circumstances of disclosure (a reasonable person would know the information was given in confidence)
- Duty of confidentiality could exist even after death – data protection only applies to living individuals

Confidentiality: Employees

- Employees are subject to an implied duty of confidentiality
- During employment - must not disclose confidential information or trade secrets
- Post employment – must not disclose trade secrets
- Confidential information - information the employer considers confidential e.g. client lists
- Trade secrets include manufacturing processes, designs, business plans etc.
  - Excludes: employee know how or public and/or trivial information
- Employers also owe their employees a duty of confidentiality

What can go wrong? Common mistakes and how to avoid them


Types of Breach 2014
140
120
100
80
60
40
20
0
Security Breach
Data sent to wrong rec.
Lost data
Emails sent to wrong rec.
Processing Breach
Failure to redact data
Loss/theft of device
Insecure disposal of papers
Info uploaded to webpage
Verbal disclosure
Incident Type


Incidents by Sector 2014
200
180
160
140
120
100
80
60
40
20
0
Health
Local Gov
Education
Lawyers
Charities
Sector

ICO Penalties

- Compensation for individuals
- ICO can impose monetary penalties – up to £500,000
- ICO can also issue the following notices:
  - Assessment – requires data controllers to comply with the principles
  - Information gathering – requires data controllers to provide information about processing
  - Enforcement – establishes whether Data Controllers have complied with the principles
- May require organisations to give undertakings promising to take action to ensure compliance with DPA

Penalties: Examples

- Norwood Ravenswood Ltd: *£70,000 for loss of highly sensitive information about care of four young children left outside London home*
- British Pregnancy Advisory Service: *£200,000 penalty after personal information was revealed to hackers*

Exercise:

- What should the British Pregnancy Advisory Service have done differently?

What are other ramifications of failing to comply with the DPA?

- Adverse publicity
- Damage to reputation
- Loss of public confidence
- May be a ‘serious incident’ requiring the Charity Commission to be notified

Steps to avoid mistakes

A. Tell people what you are doing with their data e.g. use of privacy notices

B. Make sure staff, trustees and volunteers are adequately trained

C. Only keep information for as long as necessary – consider putting a retention policy in place.

D. Keep data accurate and up to date - consider implementing procedures for updating records/inviting the Data Subject to check information held about them

E. Adopt appropriate measures and safeguards when sharing personal data

Technical and organisational measures

What measures can be taken to protect information?

- Restrict access to Personal Data
- Ensure personal data is encrypted/password protected
- Ensure anti-virus protection/firewalls are regularly updated
- Shred confidential documents
- Back-up systems to prevent data being lost
- Ensure building is equipped with physical anti-theft measures
- Ensure passwords are routinely changed
- Implement a remote working policy
- Provide staff with regular training
- Have a process in place for dealing with breaches

Social Media

- Tweets/retweets/Facebook posts – potentially defamatory
- Staff may post/tweet on behalf of the organisation from its social media accounts
- Libel requirements:
  - defamatory statement causing serious harm to reputation
  - identifying/referring to claimant
  - publication to a third party
- McAlpine v Bercow [2013]

Key Issues and Developments

- Outsourcing and instructing external contractors e.g. Payroll
- Pensions
- Shared Parental Leave
- Criminal Records Checks
- Subject Access Requests
- TUPE

Questions?

Contact Details

David Mears

Partner

020 8394 6484

David.Mears@russell-cooke.co.uk

Hannah Lyons

Associate Solicitor

020 8394 6493

Hannah.Lyons@russell-cooke.co.uk