Information Policy & Compliance

Data Protection Training

BBC

Lucy McGrath and Polly Ralph

Aims for session

- I understand how data protection impacts the BBC
- I can distinguish between personal data and sensitive personal data, data controller and data processors
- I understand the 8 data protection principles
- I know my responsibilities in relation to information security
- I understand who to contact about data security breaches and data protection generally

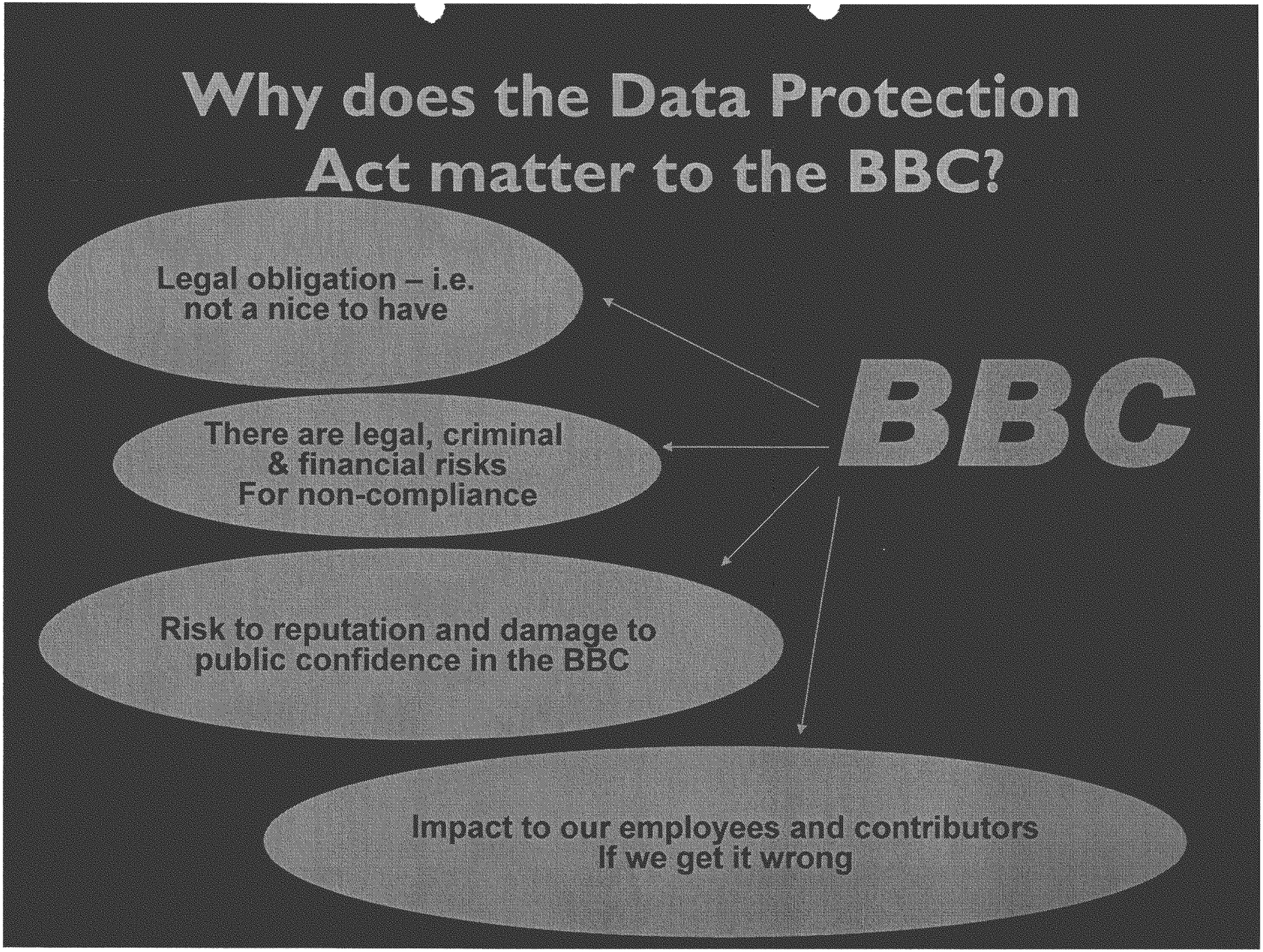
The Data Protection Act

- Data Protection Act ("DPA") does not mention "privacy"
- But – sets out manner in which organisations must protect and process personal information
- Complying with the DPA helps protect privacy

Aim of the Data Protection Act 1998

Protects legal rights of living Individuals (these people are called "data subjects") about how their Personal data is processed

Check out the BBC's DP Handbook


Why does the Data Protection Act matter to the BBC?
Legal obligation – i.e. not a nice to have
There are legal, criminal & financial risks For non-compliance
BBC
Risk to reputation and damage to public confidence in the BBC
Impact to our employees and contributors If we get it wrong

What is Personal Data?

- any information that can identify an individual
- name, address etc
- "jigsaw effect"
- What sort of personal data do you want to collect?
- What sort of personal data does the BBC hold about us as employees?

Sensitive Personal Data

These are pieces of personal data that require extra special consideration.

Individuals need to *explicitly* consent to use of sensitive personal data…. More about consent later.

What do YOU think would be *sensitive* personal data?

Sensitive Personal Data

Race

Political opinions

Religious opinions

Trade union membership

Health status

Sex life

Criminal convictions (alleged or otherwise or proceedings pending)

What sensitive personal data does the BBC collect?

What sensitive personal data might you collect?

Pick a Box

Please place the data into the correct box

Personal data

Not personal data

Sensitive personal data

More Definitions...

Data Controller

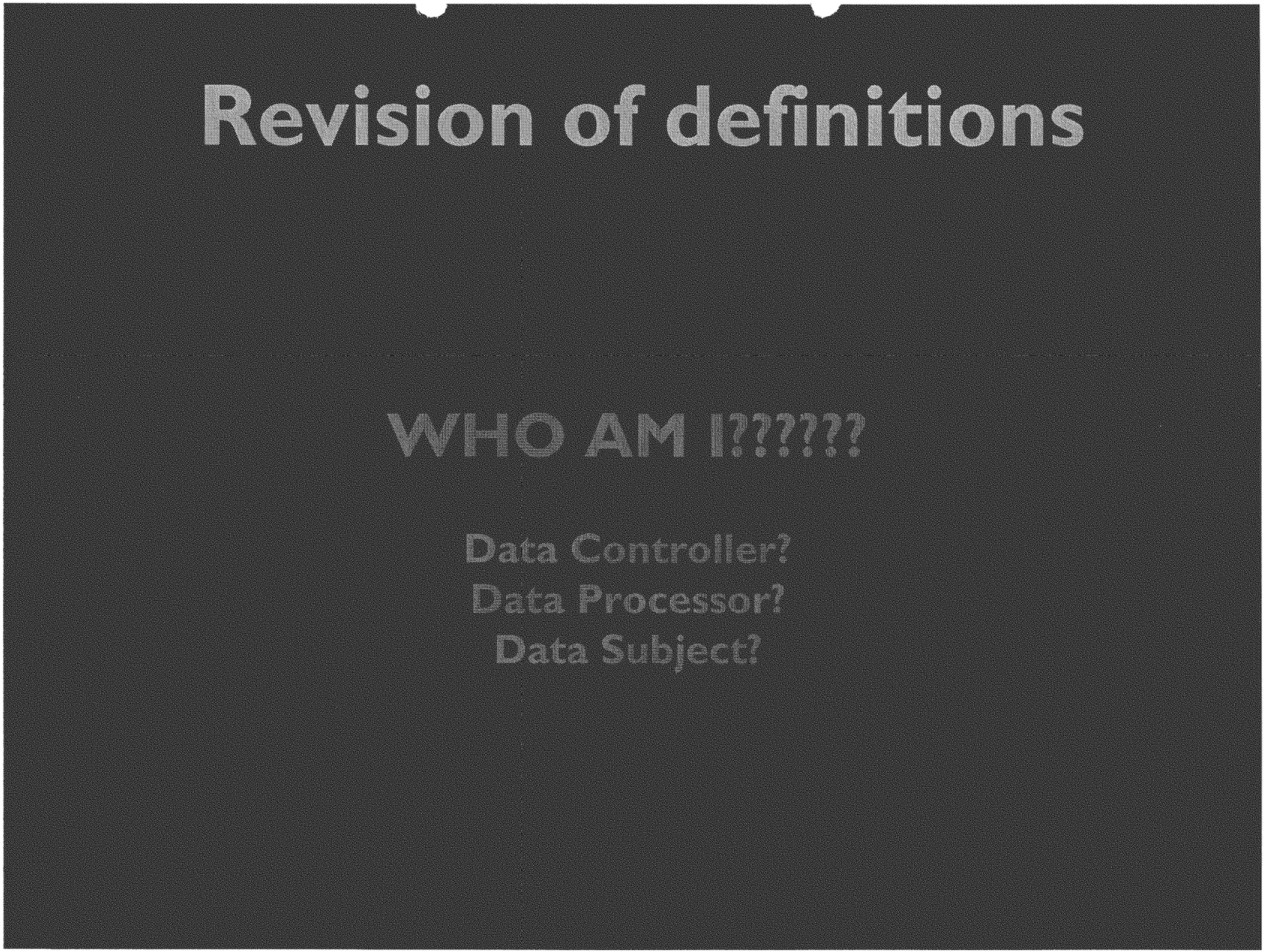
The person (usually a company) that controls how the data is collected and used

Data Processor

Processes data on behalf of Data Controller

When does BBC use data processors?

Why? What are the risks of allowing other people to process personal data?


Revision of definitions
WHO AM I??????
Data Controller?
Data Processor?
Data Subject?

Revision of definitions

Independent companies making programmes for BBC

Data Controller?

Joint Data Controller?

Data Processor?

Or Data Subject?

Revision of definitions

Me, when I ring up BBC HR Direct

Data Controller?
Data Processor?
Or Data Subject?

Revision of definitions

Siemens providing IT services to the BBC?

Data Controller?
Data Processor?
Or Data Subject?

Revision of definitions

FM & T collecting data about iPlayer usage?

Data Controller?

Data Processor?

Or Data Subject?

Review Point

We've looked at:

- What is DP?
- Definitions of data controller, processor and subject
- What is processing?

Next:

- Rules that underpin how we must deal with personal data
- How the BBC programme makers are sometime exempt from some provisions of the Data Protection Act
- Structure of data protection at the BBC

Data Protection Principles

Fair and lawful use

Accurate, and where necessary, kept up to date

In accordance with individual rights

Relevant, adequate and not excessive

Not kept longer than necessary

Expected purposes only

Security measures

Safe transfers overseas

Data Protection Principles

1. "Fair and Lawful Use"

4 Elements to be satisfied:

a) Processing must be FAIR – people should know how and why their data is being processed

b) Processing must be LAWFUL

c) One Schedule 2 condition must be satisfied

d) One Schedule 3 condition must be satisfied in relation to sensitive personal data

Data Protection Principles

1. "Fair and Lawful Use"

4 Elements to be satisfied:

a) Processing must be FAIR

- People should not be MISLED or DECEIVED as to the purposes of the processing
- Data controllers must advise: identity of the data controller, information about how the data is to be processed and any other information to ensure the processing is fair – FAIR COLLECTION NOTICE
- Processing must be LAWFUL – does what it says on the tin – we can not process data in breach of other laws – eg we could not market to people whose names had been provided on a stolen contact list

Data Protection Principles

1. "Fair and Lawful Use"

4 Elements to be satisfied:

c) Schedule 2 conditions

- Consent, necessary for a contract, compliance with the law, vital interests, necessary for justice, other legitimate purposes

c) Schedule 3 conditions for sensitive personal data

- explicit consent, employment law, vital interests, already made public by individual, legal proceedings, justice

Data Protection Principles

2. "Expected purposes only"

Obtained for specified and lawful purposes

- You must only use the data for the purposes for which it was first collected.
- Can not use Help Scheme data to market BBC programmes

Data Protection Principles

3. Relevant, adequate and not excessive.

- We must only COLLECT the minimum information required – no speculative data (even if voluntary).
- Information must, however, be ADEQUATE…. "John Smith"
- When completing a credit card application is it appropriate to ask for:
  - Home address?
  - DOB?
  - Number of sexual partners?
- Must only disclose MINIMUM information necessary – eg Help Scheme does not need to provide service providers with information about TVL payment plans

Data Protection Principles

4. Accurate and up to date

Out of date information or inaccurate information can cause a huge amount of distress (eg classification of alcoholic on NHS databases, TVL database not updated due to new partnership status)

Data Protection Principles

5. Not kept any longer than necessary.

- Ask yourself – why have we still got this data?
- Is the purpose for which it was first collected still relevant
- BBC's corporate retention policy

Data Protection Principles

6. In accordance with individual rights

Processed in accordance with the "data subject's" (the individual's) rights.

- Right to know what BBC holds
- Right to request cessation of processing that causes distress
- Right to stop direct marketing

Individuals have a right to know what data we hold!

Any person can write to the BBC, prove their identity and BBC must provide them all the information we hold about them (subject to payment of a £10 fee and certain exemptions).

This is known as a "Subject Access Request"

We only have **40 days** to respond to these.

The act requires the requester to give us reasonable assistance in locating the information.

Data Protection Principles

7. Security Measures

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Information Security

Split into 2 groups:

What are the main information security risks for the BBC?

- At the office
- On location
- Service Providers?

Information Security - Top Tips

Clear desk policy - leave nothing on your desk that contains any personal or confidential data

Ensure you **lock your computer** when you leave using a password protected screensaver

Don't EVER write your password on post-it notes

Lock cabinets. Every night. And at lunchtime.

Don't give your passwords to anyone

Lock confidential waste away overnight

Shred sensitive data by hand

Information Security - Top Tips

Never leave visitors alone

Challenge people not wearing passes

Keep distribution lists up to date

Only send emails to necessary people

Blind copy where possible

Always check entire email chain

IS YOUR LAPTOP ENCRYPTED?

Use private print job function for sensitive data

Only print when absolutely necessary

Be very careful about portable devices - do you *need* to take data outside of the BBC?

Data Processors

- BBC maintains legal responsibility under the DPA
- There MUST be a written contract
- There MUST be written instructions about how BBC expects the personal data to be processed (eg Technical specifications)
- BBC must CHECK their technical and organisational measures (eg Third Party Hosting Questionnaire, what DP training do they provide? How do they vet their staff? What sub-contractors do they use?

- See DP Handbook Module 8 for checklist

7th DPP

Data Security Breach Procedures

Loss/disclosure/inappropriate access or mishandling of either:

- **Large volumes of personal data (i.e. details of more than 100 individuals)**
- **Personal data that that could cause potential harm to the individuals (e.g. financial/credit card details for a small number of staff); or**
- **Particularly sensitive data for smaller volumes (e.g. medical records, contract details of key talent, contact details of anonymous sources).**

If in doubt about whether an event is a data security breach – contact IPC immediately on 02 26599.

- See DP Handbook Module 15 for checklist

Data Protection Principles

8. Safe transfers overseas

Not transferred outside the EEA unless certain conditions are fulfilled.

What happens if we do not comply with Data Protection

- Reputation impact - can you name a company who has suffered a breach recently? How do you feel about your information?
- Criminal offences – individuals can go to prison
- Regulator enforcement – Information Commissioner – see examples next page
- Employees – disciplinary offence to misuse personal data – ACCEPTABLE USE POLICY

BBC Data Protection Structure

1. Information Policy and Compliance – central team
2. Each division has a DP REPRESENTATIVE – Who is yours?
3. Each major department will have DP CONTACTS – anyone here a DP contact?

DATA PROTECTION GATEWAY SITE

http://sites.gateway.bbc.co.uk/foi/dataprotection/dpfrontpage.html

Review Point

We've looked at:

What is DP?
Definitions of data controller, processor and subject
What is processing?
Rules that underpin how we must deal with personal data
Structure of data protection at the BBC

QUESTIONS?????

Programmes and Data Protection

- Special exemption (s32) from data protection principles where BBC processes information ONLY for programme making
- Where we CAN process in compliance with act – we MUST
- Security of data is ALWAYS the law
- Speak to IPC or legal with questions

Programmes and Data Protection

3 conditions MUST be fulfilled if s32 is to be invoked:

- Process data with a view to publishing journalistic or artistic material; AND
- Publication is in the public interest (this decision is based on whether a programme is made in accordance with the BBC Editorial Guidelines); AND
- It would be **incompatible** with our journalism/art to comply with the data protection principles

Programmes and Data Protection – Incompatible?

Contributor databases – in most cases we can gather the information to keep details on contributors for future programmes in accordance with the Data Protection Principles (ie with consent of data subjects). See Contributors section of DPA Handbook – therefore often won't be incompatible – must abide by DPA

Newsgathering – incompatible to advise people of the information we are gathering for undercover operations

Other programme making – may collect sensitive personal data without getting explicit consent for its use (eg political ideology of individuals taking part on Any Questions, sexual history of contributors to Sunday Surgery) - incompatible to comply with DPA

Case Study

- Split into groups of 4 or 5
- 10 mins to respond to questions on Case Study
- Report to group afterwards

Question 1

What are the data protection-related steps to go through when contracting with a new supplier?

What do you advise them about data security breaches?

Question 2

World Service wants to conduct research on individuals' viewing habits in Europe and Asia. It wants to contact people via email and have them answer questions on a monthly basis.

- Are there any data protection issues?
- What are the issues if the World Service uses a third party to perform this function?
- What data protection principles apply?
- What process should be followed?

Question 3

Eaga's major technology supplier wants to move a server and helpdesk services to Australia. The server includes eaga's email system and all shared drives.

- Are there any data protection issues?
- What data protection principles apply?
- What process should be followed?
- If the technology supplier was going to further outsource this service to an Australian company – what would be the implications of this?

Question 4

We want to track user behaviour on World Service language sites using an analytics company.

- What are the data protection issues around this matter?
- What are the steps if we want to put a cookie on the web?
- The analytics company is in United States – what are the additional issues with this?
- The data subjects are all over the world – does this raise any issues?

To conclude...

If you have a data protection question do the following:

- Look at the Data Protection Handbook on gateway;
- Speak to the appropriate Divisional Rep or DP Contact; or
- Contact IPC

To conclude...

Contacts: see the

DATA PROTECTION GATEWAY SITE

AND!!!! Check out the BBC's DP Handbook