

Information Policy & Compliance

Data Protection

Training



Penn Jarvis

11 May 2011

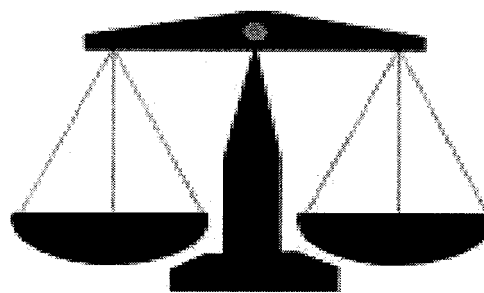
Aims for session

- 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 can identify data protection risks within my division
- I understand who to contact about data security breaches and data protection generally

The Data Protection Act 1998

The Data Protection Act (the DPA) establishes a framework of rights and duties which are designed to safeguard personal data.

Legitimate need of business
to collect and use personal
data



Right of individuals
to control what happens
to their personal data

Why does the DPA matter to the BBC?



Why does the DPA matter to you?

You (as an employee)
are a data subject –
see Module 10 of
the DPA Handbook:
how does the BBC
handle your
personal data?

Acceptable Use Policy:
Disciplinary offence to
misuse personal data

Good data protection =
more trust = more
information



The DPA applies to personal data

Personal data =

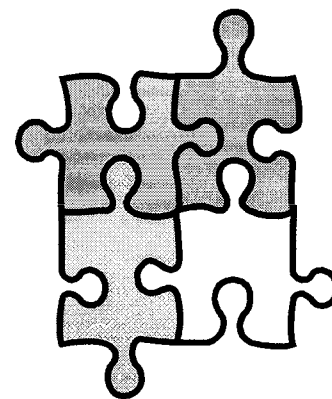
‘Data which relate to a living individual who can be identified from those data or from those data and other information which is in the possession of the data controller.’

i.e. Any information that can identify an individual and that relates to them.

When deciding whether something is personal data also consider...

- Companies are not protected by the Act (nor are people who are deceased)
- Name, address will often (but not always) be personal data
- Whether or not data is 'personal' depends on a number of factors
 - e.g.
 - Who is holding the data
 - The context in which the data is held
 - 'jigsaw effect'

IP address? Online username?
Postcode? Telephone numbers?





Sensitive Personal Data

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

Sensitive personal data attracts additional legal requirements specifically about use and its security/protection.

What do you think would be sensitive personal data?

Identify the data

Personal data

Not personal

**Sensitive
personal data**



Sensitive Personal Data

- Race or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sex life
- Criminal convictions (alleged or otherwise or proceedings pending)

What sensitive personal data does the BBC collect?



More Definitions...

Data Controller

The person (usually a company) that controls how the data is processed. Has legal responsibility for the data.

Data Processor

Processes data on behalf of Data Controller: *When does BBC use data processors?*

Processing

Pretty much anything you do with personal data is processing! Collecting, using, storing, deleting, passing to third parties etc etc....



Revision of definitions

WHO AM I??????

Data Controller?

Data Processor?

Data Subject?



Revision of definitions

Independent companies making programmes for BBC?

Me, when I ring up BBC HR Direct?

Siemens providing IT services to the BBC?

FM & T collecting data about iPlayer usage?

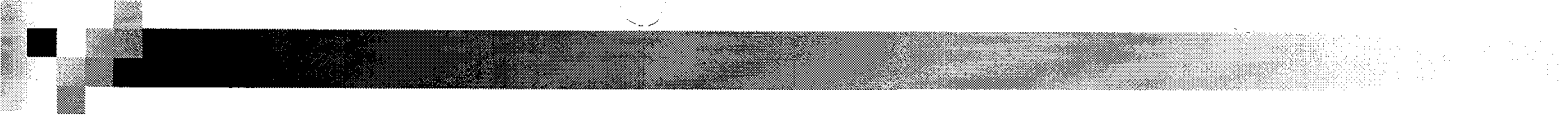
So that's **who** the DPA applies to, what about **when** it applies?



Application of the DPA

The DPA applies whenever we are processing personal data, except...

- **Section 32 exempts us from the DPA where we are processing information ONLY for Special Purposes of journalism, literature and art.**



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 special purpose (journalism/art) to comply with the data protection principles

For example:

Collecting details for contributor Database?



Is compliance with the DPA incompatible with our special purpose?



Probably not, therefore must comply with DPA

Newsgathering?



Is compliance with the DPA incompatible with our special purpose?



If yes, exempt from DPA (except for security)

Golden rule:

- Where we **can** process personal data in compliance with the DPA, we **must** (even if it's for a journalistic purpose)
- Even if we can rely on the s 32 exemption, the principle relating to **security** will **always** apply
- Speak to IPC or Legal with any questions about s 32.



Data Protection Principles

1. Processed fairly and lawfully
2. Processed for limited purposes and not in any manner incompatible with those purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than necessary
6. Processed in line with the data subjects' rights
7. Secure
8. Not transferred to countries that don't have adequate protections



Data Protection Principles

1st Principle – Personal data must be fairly and lawfully processed

FAIR processing

- People should know how and why their data is being processed
- 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 = Privacy Notice
- See Module 18 DP Handbook for guidance on drafting Privacy Notices

BBC - Radio 1 - The Chris Moyles Show - Register for Car Park Catchphrase - Microsoft Internet Explorer provided by BBC

http://www.bbc.co.uk/radio1/chris Moyles/carparkcatchphrase/

File Edit View Favorites Tools Help

Google G- Go Bookmarks 2 blocked Check AutoLink AutoFill Send to Settings

BBC NEWS | Have Your Say | Mooso - Sign-up BBC - Radio 1 - The Chris ...

BBC Text only Help Search Explore the BBC

BBC RADIO 1

Greg James
On Air Now: 13:00 - 16:00
Listen to BBC Radio 1 on FM, digital radio, digital TV and online.

Listen live Webcam Listen to a show

Home DJs & Shows Schedule News Blogs Podcasts Daytime Dance Rock/Indie Hip Hop/RnB Experimental

THE CHRIS MOYLES SHOW
Weekdays 06:30-10:00

Moyles Home | Shows | Videos | Photos | Blog | Profile | Contact

REGISTER FOR CAR PARK CATCHPHRASE

Car Park Catchphrase is BACK once again - and we want you to get involved!

The legend Roy Walker hosts the quiz where you have to guess the catchphrases from the clues.

If you'd like to take part then just fill in the form below to register.

We'll be picking people at random to take part.

Car Park Catchphrase is broadcast Monday - Thursday on the Chris Moyles show on Radio 1

start | Internet | 100% | 15:35

BBC - Radio 1 - The Chris Moyles Show - Register for Car Park Catchphrase - Microsoft Internet Explorer provided by BBC

http://www.bbc.co.uk/radio1/chris Moyles/carparkcatchphrase/

File Edit View Favorites Tools Help


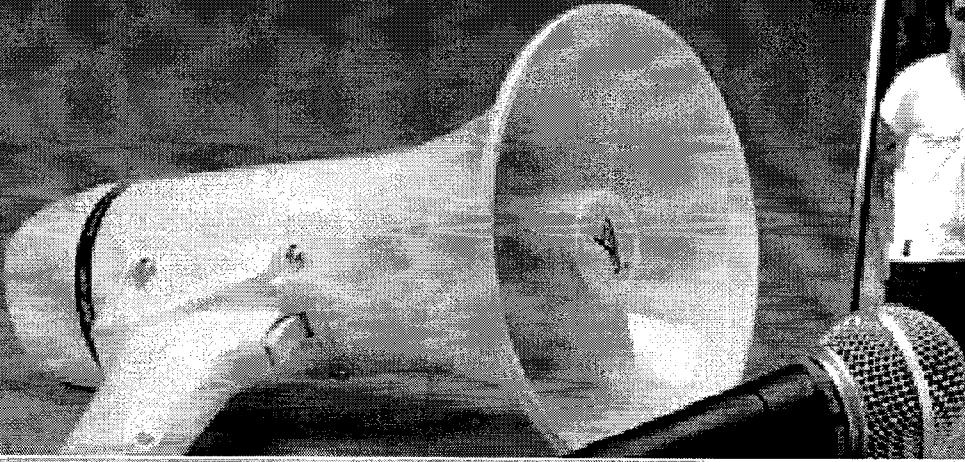
Google G Go Bookmarks 2 blocked Check AutoLink AutoFill Send to Settings

BBC - Privacy and Cookies Pg... BBC - Radio 1 - The Chris ... X

I accept the Terms & Conditions

The information you provide will only be used by the BBC to contact you if you are selected to take part in Car Park Catchphrase. If you are selected, only your name, town and car will be read out on air; your contact details will be held securely by the BBC. Please visit the BBC's [Privacy & Cookies Policy](#) for more information.

Submit



Internet 150%

start Inbox - Microsoft Out... \\bbord2013\central... Microsoft PowerPoint... BBC - Radio 1 - The C... 15:55

The screenshot shows a Microsoft Internet Explorer browser window displaying the BBC Privacy and Cookies Policy page. The browser's address bar shows the URL <http://www.bbc.co.uk/privacy/>. The page header features the BBC logo, a search bar, and a link to "Explore the BBC". The main heading is "Privacy and Cookies Policy".

Topics:

- Introduction and General Terms
- What information will the BBC collect about me?
- How will the BBC use the information they collect about me?
- When will the BBC contact me?
- Will I be contacted for marketing purposes?
- Will the BBC share my personal information with anyone else?
- Offensive or inappropriate content on the BBC website
- What if I am aged 16 or under?
- How long will the BBC keep my personal information?
- Can I find out what personal information the BBC holds about me?
- What if I am accessing BBC websites from outside the UK?
- Changes to the BBC's Privacy Policy
- Cookies Policy
- Contacting the BBC about this Privacy Policy

1. Introduction and General Terms

The right-hand sidebar contains several sections of links:

- Important notice for use**
- Targeted Advertising Update**
- General BBC information**
- What's on the BBC?**
- Free tickets to BBC shows
- How to visit the BBC
- Transcripts or recordings
- Re-use of BBC programme
- Take part in a programme
- Help receiving the BBC
- How to get digital channel
- History of the BBC
- Your licence fee and how
- Sending a programme idea
- Supplying the BBC
- Finding documents or reports

The Windows taskbar at the bottom shows the Start button, several open applications including "Inbox - Microsoft Outlook", "BBC - Privacy and Co...", and "Microsoft PowerPoint", and the system clock showing 15:56.



Data Protection Principles

1st Principle – Personal data must be fairly and lawfully processed

Lawful Processing

- We can not process data in breach of other laws
- e.g. we could not market to people whose names had been provided on a stolen contact list

Data Protection Principles

In order for processing to be fair & lawful, a condition from Schedule 2 (for standard personal data) or Schedule 3 (for sensitive personal data) must be satisfied:

Schedule 2 conditions

- Consent, necessary for a contract, compliance with the law, vital interests, necessary for justice.

Schedule 3 conditions for sensitive personal data

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



Data Protection Principles

2nd Principle “Expected purposes only”

- You must only use the data for the purposes for which it was first collected.

e.g Can not use Help Scheme data to market BBC programmes



Data Protection Principles

3rd principle: 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”
- Must only disclose minimum information necessary
- *E.g. Help Scheme does not need to provide service providers with information about TVL payment plans*



Quick Brainstorm

You're offering free tickets to a live BBC event. Members of the public sign-up, via a website. They have to provide their name, address, DOB, details of any disabilities, via the BBC website.

What information do you think you would want to include on the privacy notice?

Do you think it is ok to collect all this data?

You decide you want to contact the applicants after the event for audience research purposes. Can you do this? Is there any way you could have made this easier at the outset?



Data Protection Principles

4th Principle: Personal data must be 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

5th Principle - Personal data must not be kept longer than necessary.

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



Quick Brainstorm

You are a manager. Nine years ago, during a turbulent time in her personal life, a member of your team's behaviour resulted in you issuing formal disciplinary proceedings against her. Following this, she quickly returned to her formerly excellent standard of work.

You are going through some old personal files and you notice you still have the notes about the disciplinary matter. Is it acceptable under the DPA to destroy them?



Data Protection Principles

6th Principle: Processed in accordance with the “data subject’s” (the individual’s) rights.

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

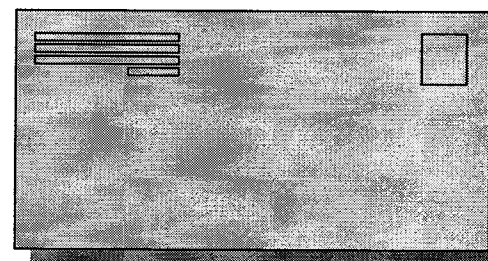
Individuals have a right to know what data we hold

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.

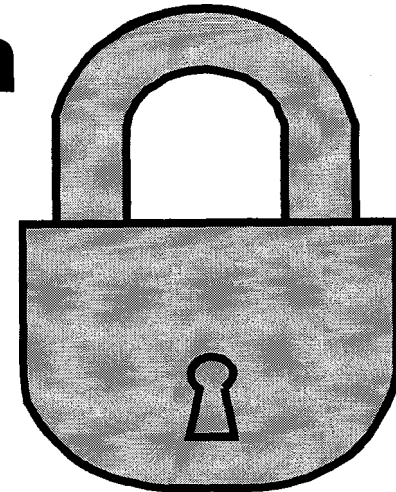
The DPA requires the requester to give us reasonable assistance in locating the information.





**Be aware that anything
you record (eg in an
email) could
potentially be released
to in response to a SAR**

Data Protection Principles



7th principle 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 – 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?

7th principle - Data Processors

Processors raise extra 7th principle risks; the data is out of our hands. But the BBC maintains legal responsibility under the DPA.

- There **MUST** be a written contract
- There **MUST** be written instructions (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



Quick Brainstorm

There have been some technical issues with software operated by the BBC.

BBC wants to export a data file (containing personal data) to an external company who will convert the data and return it back to the BBC in a usable format.

Is this okay? What do we need to do in terms of the 7th principle?

Does it matter where the external company is based?

Data Protection Principles



8. Safe transfers overseas

Personal data must not be transferred outside the EEA unless certain conditions are fulfilled.

If you want/need to transfer data outside the EEA, talk to IPC as we can help to put safeguards in place.

8th Principle



- Transfers within the BBC are treated as transfers within the EEA
- Other BBC offices are required to meet the same standards and comply with the same policies and procedures as UK offices

8th principle



If transferring to countries which are not designated safe, additional conditions must be met for example:

- Putting in place a data transfer agreement based on EC model terms
- Making a formal assessment of adequacy

If you want/need to transfer data outside the EEA, talk to IPC as we can help to put safeguards in place.



Recap: Data Protection Principles

1. Processed fairly and lawfully
2. Processed for limited purposes and not in any manner incompatible with those purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than necessary
6. Processed in line with the data subjects' rights
7. Secure
8. Not transferred to countries that don't have adequate protections

Cookies

- Must provide information about how to refuse cookies
- Must have ALL cookies registered internally



Privacy and Electronic Comms Regulations “ePrivacy”

- Additional regulations that set out rules for e-marketing via email, text etc
 - Also regulate how to deploy cookies
 - **Must have opt-in consent to market via email/text**
 - **Consent is a positive act – ticking a box, sending an email, clicking an icon**
 - **Subscribe to marketing boxes should not be pre-ticked**
 - **Must provide free mechanism to unsubscribe with every message (even texts)**
 - **£500k fine for serious breach of the ePrivacy Regulations**
-
- Transparency
 - Control



Question 1

June, who works for BBC Pensions, receives a call from John. John wants to know how much money is in his wife, Sheila's, pension fund. He explains that Sheila has not been at the office for the past few weeks as she has been in isolation in hospital after contracting MRSA. It's not looking good for Sheila, and John is trying to work out what the family's financial situation would be if Sheila dies.

June takes full notes of the call, including John's full name and address and mobile number.

Should June give John the details of Sheila's account?
What data protection principles apply?

June's partner, Marjorie, has just started work at a law firm that specialises in taking action against hospitals on behalf of family members of MRSA victims. June passes on John's details to Marjorie telling her that she should get in touch with John as he might be needing her legal services.

- What data protection principles apply?
- Who is/are the data subjects?



Question 2

James is a member of the finance team within BBC Finance. A freelance colleague suggests that he and James conduct a search on the BBC Finance system to see how much a Newsnight presenter gets paid compared to someone who hosts a show.

James believes that conducting this search could further his knowledge of talent fees, which might be able to assist him in the future. He agrees to conduct the search on the proviso that the data wouldn't go outside the BBC.

What's the personal data at issue?

What's the harm that could come from disclosing data?

What data protection principles are relevant?

What BBC policies are relevant to this scenario?



Question 3

A company that provide text messaging services for BBC Wales has just contacted you telling you about the loss of a laptop.

It was held by a sub-contractor of theirs and includes all the phone numbers and texts of audience members who had texted into a Welsh Radio competition 12 months ago.

The competition asked viewers to provide their age and name.

What questions would you ask the company?

In your view, is this a data security breach? Why/Why not?

What steps would you take to address this situation?



Data Security Breach Procedures

BBC defines a data security breach as loss/disclosure/inappropriate access or mishandling of:

- personal data; or
- highly commercially sensitive data relating to the BBC and/or its suppliers.

Data Security Breach Procedures

Miskandling

Inappropriate
Access

Disposal

Data Security breach procedures

BBC defines a 'serious incident' as a data security breach that involves the loss/disclosure/inappropriate access or mishandling of either:

- Large volumes of personal data (ie details of more than 100 individuals)
- Personal data that that could cause potential harm to the individuals (eg financial/credit card details); or
- Highly commercial sensitive data which could cause significant harm to the BBC or another company
- Particularly sensitive data (eg medical records, contract details of key talent, contact details of anonymous sources);
- Personal data relating to children.

See DP Handbook Module 15 for procedure

If you suffer a breach contact Ext
26599 IMMEDIATELY

BBC NEWS | Northern Ireland | Thousands of driver details lost - Microsoft Internet Explorer provided by the BBC

http://news.bbc.co.uk/1/hi/northern_ireland/7138408.stm

File Edit View Favorites Tools Help

Google G- Go Bookmarks 0 blocked Check AutoLink AutoFill Send to Settings

BBC NEWS | Northern Ireland | Thousands of driver d... Page Tools

BBC Home Search Explore the BBC

Low graphics | Accessibility help

BBC NEWS **LIVE LIVE** BBC NEWS CHANNEL News services Your news when you want it

News Front Page World UK England Northern Ireland N Ireland Politics Scotland Wales Business Politics Health Education Science & Environment Technology Entertainment Also in the news Video and Audio Have Your Say Magazine In Pictures Country Profiles Special Reports

RELATED BBC SITES

Last Updated: Tuesday, 11 December 2007, 15:55 GMT

E-mail this to a friend Printable version

Thousands of driver details lost

The Driver and Vehicle Agency in Northern Ireland has lost the personal details of 6,000 people.



The data was on two discs and went missing after being sent to the agency's headquarters in Swansea.

The DVA said the data was being provided in response to a safety recall by a number of manufacturers.

The head of the agency said the information was not encrypted. It included details of 7,685 vehicles and more than 6,000 vehicle keepers.

The data includes the keeper's name, address, registration mark of the vehicle, chassis number, make and colour.

However, the DVA said no personal financial data was on

VIDEO AND AUDIO NEWS
DVA chief executive Brendan Magee apologises for the loss
Watch

BENEFIT DISCS LOST

KEY STORIES

- Discs loss 'entirely avoidable'
- MoD 'Facebook generation' fear
- New boss for HMRC after data slip
- Tougher data rules for Whitehall
- More firms 'admit disc failings'
- £20,000 reward offered for discs
- Fresh benefit data lapse admitted
- Discs 'worth £1.5bn' to criminals

Queries answered
BBC personal finance reporter Jennifer Clarke answers your questions on the crisis

FEATURES AND BACKGROUND

- Q&A: Child benefit records lost
- Government letter: full text

“ It wasn't encrypted - this ”

Internet 100%

start Microsoft Office 2 Windows Explorer 2009-12-01 PR - Scot... BBC NEWS | Northern... 10:35

BBC NEWS | Politics | Discs loss 'entirely avoidable'
BBC Low graphics Help Search Explore the BBC
NEWS 

- News Front Page
- World
- UK
- England
- Northern Ireland
- Scotland
- Wales
- Business
- Politics**
- Health
- Education
- Science & Environment
- Technology
- Entertainment
- Also in the news
- Video and Audio
- Have Your Say
- Magazine
- In Pictures

Page last updated at 18:41 GMT, Wednesday, 25 June 2008 19:41 UK

E-mail this to a friend Printable version

Discs loss 'entirely avoidable'

The loss of discs containing personal details of 25 million people was "entirely avoidable", a report says.

The Poynter report does not blame individual officials, but highlights "serious institutional deficiencies" at HM Revenue and Customs (HMRC).

Chancellor Alistair Darling told MPs action was already being taken to improve data security.

The Tories said the report and another by the Independent Police Complaints Commission were "truly devastating".

Shadow Chancellor George Osborne said they highlighted



Alistair Darling's statement to the Commons

BENEFIT DISCS LOST

- KEY STORIES
- ▶ Discs loss 'entirely avoidable'
 - ▶ MoD 'Facebook generation' fear
 - ▶ New boss for HMRC after data slip
 - ▶ Tougher data rules for Whitehall
 - ▶ More firms 'admit disc failings'
 - ▶ £20,000 reward offered for discs
 - ▶ Fresh benefit data lapse admitted
 - ▶ Discs 'worth £1.5bn' to criminals

Queries answered
BBC personal finance reporter Jennifer Clarke answers your questions on the crisis

BBC NEWS | Politics | Discs 'worth £1.5bn' to criminals - Microsoft Internet Explorer provided by the BB

http://news.bbc.co.uk/1/hi/uk_politics/7117291.stm

File Edit View Favorites Tools Help

Google G Go Bookmarks 0 blocked Check AutoLink AutoFill Send to Settings

BBC NEWS | Politics | Discs 'worth £1.5bn' to criminals

BBC Home Search Explore the BBC

Low graphics | Accessibility help

BBC NEWS LIVE BBC NEWS CHANNEL

News services
Your news when you want it

News Front Page
World
UK
England
Northern Ireland
Scotland
Wales
Business
Politics
Health
Education
Science & Environment
Technology
Entertainment
Also in the news

Video and Audio
Have Your Say
Magazine
In Pictures
Country Profiles
Special Reports


RELATED BBC SITES
SPORT

Last Updated: Wednesday, 28 November 2007, 16:12 GMT

E-mail this to a friend Printable version

Discs 'worth £1.5bn' to criminals

Two missing computer discs containing the personal details of 25 million people could be worth up to £1.5bn to criminals, say the Lib Dems.



Mr Cable said the discs could dwarf the value of the Brinks Mat robbery

Acting leader Vincent Cable told MPs an "enormous amount" was still at stake, after discs containing the entire child benefit database got lost in transit.

Ministers say there is no evidence they have been intercepted by criminals.

But in a Tory-led debate on the issue shadow chancellor George Osborne asked if the "whole truth" had been told.

The discs were lost after HM Revenue and Customs sent discs to the National Audit Office unregistered and unencrypted.

BENEFIT DISCS LOST

KEY STORIES

- Discs loss 'entirely avoidable'
- MoD 'Facebook generation' fear
- New boss for HMRC after data slip
- Tougher data rules for Whitehall
- More firms 'admit disc failings'
- £20,000 reward offered for discs
- Fresh benefit data lapse admitted
- Discs 'worth £1.5bn' to criminals

Queries answered

BBC personal finance reporter Jennifer Clarke answers your questions on the crisis

FEATURES AND BACKGROUND

- Q&A: Child benefit records lost
- Government letter: full text
- Taking cover from ID theft
- Point-by-point: Darling statement
- The dealers in data
- Life inside the beleaguered HMRC
- Timeline: Benefits records loss

Done Internet 100%

start Microsoft Office O... 2 Windows Explorer 2009-12-01 PR - Scot... BBC NEWS | Politics | ... 10:36



Low graphics Help

Search

Explore the BBC

NEWS

LIVE BBC NEWS CHANNEL

Page last updated at 21:11 GMT, Tuesday, 17 November 2009

E-mail this to a friend Printable version

- News Front Page
- World
- UK**
- England
- Northern Ireland
- Scotland
- Wales
- Business
- Politics
- Health
- Education
- Science & Environment
- Technology
- Entertainment
- Also in the news
- Video and Audio
- Have Your Say
- Magazine
- In Pictures

T-Mobile staff sold personal data

Staff at mobile phone company T-Mobile passed on millions of records from thousands of customers to third party brokers, the firm has confirmed.

Details emerged after the firm alerted the information commissioner, who said his office was preparing a prosecution.

Christopher Graham said brokers had sold the data to other phone firms, who then cold-called the customers as their contracts were due to expire.

A T-Mobile spokesman said the data had been sold "without our knowledge"



Information Commissioner: "The penalties... aren't strong enough to stop it"

- SEE ALSO
- Calls to tighten data abuse laws 05 Sep 09 | UK
 - NHS told to tighten data security 25 May 09 | UK
 - Ex-BNP man fined over names leak 01 Sep 09 | Nottinghamshire

- TOP UK STORIES
- British yachtsmen freed by Iran
 - Nato must follow US example - PM
 - Building societies agree merger

News feeds

MOST POPULAR STORIES NOW

BBC News - First Data Protection Act fines issued by commissioner - Microsoft Internet Explorer provided by the BBC

http://www.bbc.co.uk/news/uk-11821203

File Edit View Favorites Tools Help

! (0 unread) Yahoo! Mail, plkn... Ico fines BBC - Google Search BBC News - First Data Pr...

BBC Mobile News Sport Weather iPlayer TV Radio More Search BBC News

NEWS UK

Home World UK England N.Ireland Scotland Wales Business Politics Health Education Sci/Environment Technology Entertainment & Arts

24 November 2010 Last updated at 12:18

First Data Protection Act fines issued by commissioner

A county council that faxed details of a child sex abuse case to a member of the public is to be fined £100,000 for breaching the Data Protection Act.

Hertfordshire County Council is one of two bodies fined by the Information Commissioner - both have apologised.

Sheffield-based A4e was fined £60,000 for losing an unencrypted laptop with the details of thousands of people.

The commissioner said the fines - the first he has issued - would "send a strong message" to those handling data.

Commissioner Christopher Graham was granted the authority to serve financial penalties for data protection breaches in April of this year.

Fax mistakes

The breaches at Hertfordshire County Council occurred in June, when employees in the childcare litigation unit accidentally sent two faxes to the wrong recipients on two separate occasions. The council reported both breaches to the Information Commissioner's Office (ICO).



A company's employee took home a laptop containing personal information about 24,000 people

Related stories

- Privacy code of practice issued
- NHS 'worst for breaches of data'

Top Stories

- Tobacco displays facing shop ban
- Libyans 'will fight' no-fly zone
- BOA Olympic cash row intensifies
- Special needs 'help for families'
- Council tax 'to fall this year'

Features & Analysis

- Gas muzzlers: Is saving fuel the new driving obsession?
- Peas are good: Spuds, neeps, leeks - just what is the UK's national vegetable?
- WAL*MART: Sex and the payslip: The women accusing the world's biggest retailer of discrimination
- In pictures: Ten years after destruction of Afghanistan's Bamian Buddhas

start | Inbox - Microsoft Out... | BBC News - First Dat... | Corporate Centre | Microsoft PowerPoint | Internet | 100% | Links | 14:11



ICO Fines issued

Hertfordshire County Council = fine of £100,000

- 2 faxes sent to the wrong number on 2 occasions
- Information = sensitive personal data about child sex abuse cases.
- How easy is it to send an email to the wrong address?

A4e = fine of £60,000

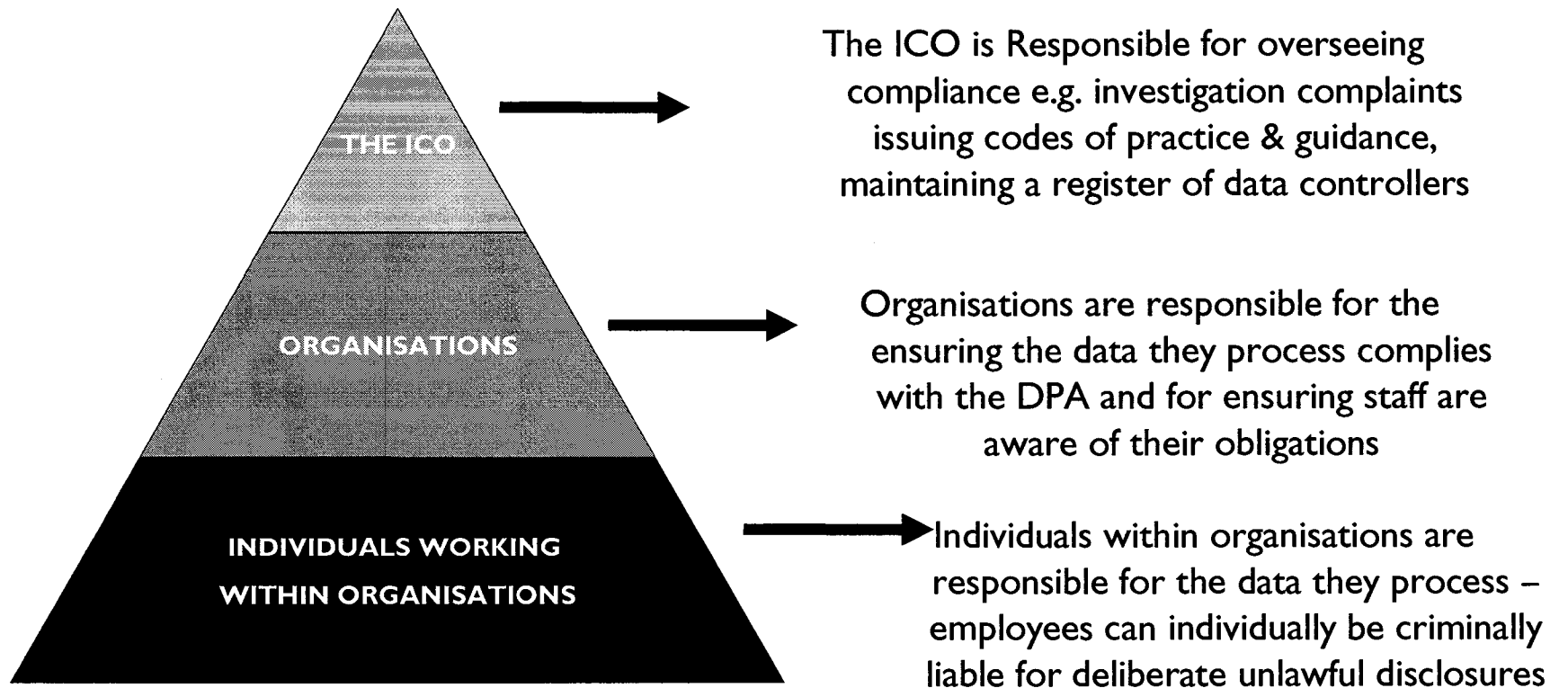
- Laptop containing personal information relating to 24,000 people who had used community legal centres.
- Laptop was unencrypted and stolen from the employee's home

ICO Fines issued

Ealing Council = fine of £80,000 & Hounslow Council = £70,000

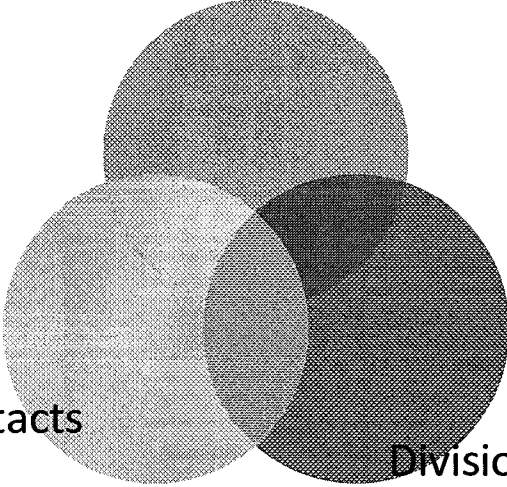
- Personal details of 1,700 individuals were lost when the **laptops** were stolen from one of the employee's home.
- Both councils have a policy on encryption but the laptops were unencrypted.
- The ICO says that Ealing Council was in breach of its own **policy** as it was **not checking** that it was followed or understood by staff.
- Hounslow Council breached the Act by **failing to have a written contract** in place with Ealing Council. Also, Hounslow did **not monitor** Ealing Council's procedures for **operating the service securely**.
- These fines follow a similar incident last year (loss of unencrypted laptop) which led to a £60,000 fine against an employment advice firm A4e.

Who is responsible for DP compliance?



BBC Data Protection Structure

Information Policy & Compliance: IPC Adviser for each Division (see Gateway).



Data Protection Contacts
within each Department

Divisional DP Representative



To conclude...

The BBC (and that means all of us):

- must comply with the 8 Data Protection Principles. The consequences of not doing so may be severe.
- is responsible for all its data processing; including that done by 3rd parties



To conclude...

If you have a data protection question, do the following:

- Look at the Data Protection Handbook on Gateway;
- Speak to your Divisional Rep or a DP Contact within your department; or

■ Contact us!

Details on the Information Policy & Compliance Gateway page



Thank you!

Penn Jarvis

Ext: (02) 25646

Penn.jarvis@bbc.co.uk