

BYOD and CMPs

Michele Harmer

Lead Policy Officer, Public Security

20 September 2012

ico.

Information Commissioner's Office

The role of the ICO

- Enforce and regulate
 - Freedom of Information Act
 - Data Protection Act
 - Environmental Information Regulations
 - Privacy and Electronic Communications Regulations
- Provide advice to individuals and organisations
- Adjudicate on complaints
- Promote good practice

European Commission's proposal for a new general Data Protection Regulation

- The ICO's initial response (Jan 2012) to the Commission's proposal is available at: www.ico.gov.uk
- The Ministry of Justice did a call for evidence on the new legislative proposals which closed 6 March 2012. The report is available on their website.
- The Justice Select Committee, chaired by Sir Alan Beith MP, have also called for evidence for its inquiry into European Union Data Protection Framework Proposals.
- **Next steps:** this is the start of the process towards a change in the law which will be negotiated in the European Council and Parliament. Changes to the law are likely to take at least a couple of years after this date to agree and a timetable for implementation will then be required.

BYOD – Bring Your Own Device

What are the risks?

- Lack of control
- The type of data held/accessed
- Transferring the data
- Device security
- Dealing with breaches.

BYOD Top Tips

- Use a strong password to secure your devices. Avoid the use of 4-digit PINs – they are often easy to guess
- Enable file encryption to encrypt data stored in the device securely
- Ensure that access to the device is locked or data automatically deleted if an incorrect password is input too many times
- Ensure that the device automatically locks if inactive for a period of time
- Make sure users know exactly which data will be automatically or remotely deleted and under which circumstances
- Maintain a clear separation between the personal data processed on behalf of the data controller and that processed for the device owner's own purposes

Other considerations?

- Don't forget compliance with all DPA principles.
- Compliance with Subject Access Requests.
- Compliance with FOI Requests.
- Other legislation?

ICO powers and penalties

- Undertakings;
- Enforcement Notices;
- Civil Monetary Penalties;
- Audit (non-compulsory unless Cent. Govt);
- No further action / recommendations....*but*...we expect these to be acted upon

Monetary penalty powers

- Significant losses of personal data from 2007, existing powers deemed inadequate
- New power inserted into section 55 of Data Protection Act 1998 by section 144 of the Criminal Justice and Immigration Act 2008 (CJIA)
- The Commissioner determines the penalty and specifies the amount in a notice to the data controller. (maximum £500,000.)
- The penalty is paid into the Consolidated Fund owned by HM Treasury

Specific requirements

- The ICO has to be satisfied that:
 - There has been a **serious** contravention of data protection principles by the data controller,
 - The contravention was of a kind likely to cause substantial damage or substantial distress **and** either...
 - The contravention was deliberate **or**,
 - The data controller knew or ought to have known that there was a risk that the contravention would occur, **and** that such a contravention would be of a kind likely to cause substantial damage or substantial distress, **but** failed to take reasonable steps to prevent the contravention.

Monetary penalties

- Over 700 cases investigated 2011/2012 across a range of sectors;
- 22 monetary penalty notices issued to date
- Local government and health predominate – there is an expectation upon the NHS to report sufficiently serious incidents to the ICO proactively;
- Predominantly principle seven issues to date, however elements of principle four (accuracy) and principle five (retention);
- The 'breach' may be the failure of the data controller to take appropriate technical or organisational steps to protect data, rather than the incident itself.

Case studies

£60,000

St George's Healthcare NHS Trust:

- Two letters sent to the wrong address containing highly sensitive personal data.
- DS had provided new details & old address was 5 years out of date.
- The NHS have one central database containing all patient details and separate local administration database.
- Two secretaries, both trained, compiled the data without checking the local database.
- DC was aware that staff could bypass database prompt and that using the system was difficult and cumbersome.

Case studies

£150,000

Welcome Financial Services Ltd:

- The DC's IT team maintained back-ups of the Local Area Network each day. The tapes used to back-up were daily transported from the IT secure room and re-used.
- Two tapes went missing containing 20,000 personal details of staff members. The details included bank account details, CV's, National Insurance numbers and 510,000 customer details.
- Both tapes weren't recovered and were not encrypted which breached the DC's security policy.

Case studies

£325,000

Brighton and Sussex University Hospitals NHS Foundation Trust:

- The DC's data processor hired a third party to destroy hard drives without DC knowledge.
- The third party sold four of the 'destroyed' hard drives to a data recovery company who discovered the data.
- Data recovered included two substantial databases which could be linked containing details of 67,642 patients and 1527 HIV positive patients.
- DC assured the ICO that only these hard drives had been compromised, however 15 more were later found containing data.

Self reported breaches

- Themes emerging;
 - Unencrypted devices (loss and theft);
 - Insecure disposal (both paper and electronic);
 - Email errors;
 - Fax errors;
 - Postal errors;
 - Loss or theft of paper records.

Managing an incident

- Have a breach management plan in place. Ensure that relevant staff know what this is, where they can access it and how it affects them. Clearly define roles and responsibilities;
- Containment and recovery. Could it happen again? What steps can you take straightaway to prevent this?
- Informing and managing affected data subjects. Is it appropriate to inform?
- Notification of breach – failure to report may be considered an aggravating factor.

Reporting an incident

- The ICO has produced a form to assist:



Security breach notification form

This form is for data controllers to report a breach of security to the ICO. It should take about five minutes to complete.

Before completing this form, you should read the following guidance: [Notification of Data Security Breaches to the Information Commissioner's Office](#).

Please provide as much information as possible. If you don't know the answer, or you are waiting on completion of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant information, eg incident reports.

1	What is the name of your organisation (the data controller)?	
2	Who should we contact if we require further details concerning the incident? (Name and job title, email address, contact telephone number and postal address)	
3	Have you notified as a data controller? If so please provide your registration number. Search the online Data Protection Public Register .	
4	Have you reported any previous incidents to the ICO? If so, please provide brief details and reference numbers, where known.	
5	When did this incident occur?	
6	Please briefly describe the incident.	
7	Has any personal data been placed at risk? If so, please give us an outline of what this data consists of.	
8	Approximately how many data subjects have been affected?	
9	Have you informed the data subjects that this incident has occurred?	
10	Has there been any media coverage of	

the incident?		
11	Have you taken any action to minimise/mitigate the effect on the data subjects involved? If so please provide brief details.	
12	Are you carrying out an investigation into the incident - If so when will you complete it and what format will it take?	
13	Have you informed any other regulatory body of the matter? If so please provide their details and an outline of their response.	
14	What action have you taken to prevent similar incidents in the future?	
15	Is there any other information you feel would be helpful to the ICO's assessment of this incident?	

Sending this form
Send your completed form to casework@ico.gsi.gov.uk, with 'Security breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please note that we cannot guarantee security of forms sent by email.

What happens next?
When we receive this form, we will contact you within seven calendar days to provide:

- a case reference number; and
- an explanation of what to expect during our investigation of the incident.

If you need any help in completing this form, please contact our helpline on **0303 123 1113** or **01625 545745** (operates 9am and 5pm Monday to Friday).

http://www.ico.gov.uk/for_organisations/data_protection/lose.aspx

What to expect

- An acknowledgement with a unique case reference number;
- An explanation of our powers;
- A designated contact name and contact details on allocation;
- A chance to explain what has happened, why and any remedial steps taken;
- Regular communication;
- Careful consideration of the facts of the case

Keep in touch

Subscribe to our e-newsletter at www.ico.gov.uk
or find us on...

