

Fine by me

A commentary of the ICO's recent monetary penalties

Under sections 55A and 55B of the Act the Commissioner may serve a monetary penalty notice on a data controller requiring the data controller to pay up to £500,000.

The Commissioner has to be satisfied that

“... there has been a serious contravention of section 4(4) of the Act by the data controller (that's the principles) and it was of a kind likely to cause substantial damage or distress, and it was deliberate and the data controller should have known that there was a risk and failed to take reasonable steps to prevent it”

The first two such penalties were announced on 24th November 2010.

On 11 June 2010 a member of staff at the Childcare Litigation Unit of Hertfordshire County Council sent 17 pages of confidential and sensitive personal data by fax to a member of the public instead of to a barrister's Chambers. The documents related to a sexual abuse case involving a child which was being heard at the High Court. The member of staff had input the wrong STD code for Chambers and also failed to use a fax header sheet which would have provided an unintended recipient with details of the sender and instructions on what to do with a misdirected fax.

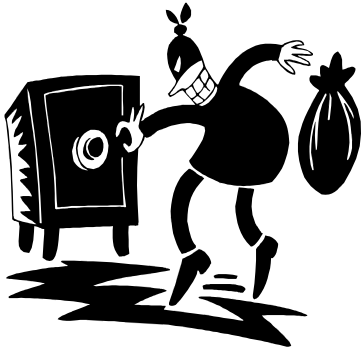
Subsequently both the data controller and the member of the public reported the security breach to the Commissioner's office. The Commissioner was so concerned about the security breach that two members of staff from the Enforcement team went to the data controller's premises on 24 June 2010 to meet with senior managers.

On the very day the Commissioner was talking to their management team another member of staff in the Childcare Litigation Unit sent 11 pages containing confidential and sensitive personal data by fax to the wrong number instead of the intended recipient of Watford County Court. This time they remembered the fax header and the breach was contained.

The council didn't seem to have any common sense policies in place such as “Ring ahead” or “Confirm receipt” and there seemed to be a reluctance to use these methods. The outcome was £100,000 and the perpetual notoriety of being the first to be fined. (Trivial Pursuit IPR & Privacy version 2015).



The other fine in November 2010 was to a company called A4e in Sheffield which processes data for amongst others the Legal Services Commission. An employee took home a laptop to work on the data. The only security on the laptop computer was password protection.



On the night of 18th June 2010 the employee was burgled at home with the loss of the laptop holding the sensitive personal data relating to 24,000 clients.

The data included the case type such as debt, welfare, employment, the name, postcode, date of birth and gender of the data subject together with whether or not the data subject was a lone parent, care leaver, carer, a victim of violence, ex-offender, young offender or gypsy traveller.

There was no record of any staff induction training being held although staff had been issued with a selection of policies. Guidance had also been issued to lock laptops away when not in use. The employee left it on a dining table in plain view. Remedial action at this company include mandatory IT security training.

8th February this year saw 2 more fines for 2 more Councils.

Two laptops containing the details of around 1,700 individuals were stolen from an employee's home. Almost 1,000 of the individuals were clients of Ealing Council and almost 700 were clients of Hounslow Council. Both laptops were password protected but unencrypted - despite this being in breach of both councils' policies. Social Care is the sector.

This was complicated by the fact that Hounslow Council breached principle 6 of the Act by failing to have a written contract in place with Ealing Council. Hounslow also did not monitor Ealing Council's procedures for operating the service securely. Data Controllers who engage data processors to work on their data need a written contract in place and to monitor that contract.

The Commissioner also decided that 3rd principle (adequacy) and 5th principle (retention) had been breached. The data wasn't relevant and had been kept way past its use by date.

Analysing these 4 cases leads to some interesting conclusions. Firstly 3 of the 4 involve laptops which were merely password protected. The laptops were stolen from employee's



homes. The data wasn't encrypted despite it being social care and child abuse data which certainly fits into my Schedule 3.

Moral - don't work from home. If your boss makes you work from home then lock your doors and keep your laptop under your pillow when you finish work. Dining room tables are just not quite secure enough. And finally - get encrypted.

The other case falls into the category of 'you couldn't make it up...'

An employee tried to use a preset fax number but it was busy so typed in the number themselves and got it wrong. Then when the regulator was dunking his biscuits a week or so later and talking about the cock up another employee did exactly the same thing. They forgot the fax header sheet. They never thought to ring ahead and say a fax is on the way. They just went ahead and did it.

Act Now was at a meeting recently where an ICO speaker talked about monetary penalties and gave us the hard word. He didn't quite wag his finger but he made it clear that they were getting tough. He also said that the onus was on data controllers to self report any significant breaches of the Act and that trying to sweep it under the carpet would result in tougher sanctions. A press release in January 2010 said

“Over 800 data security breaches have been reported to the Information Commissioner's Office in just over two years. The ICO is warning that organisations may face tougher sanctions if they fail to report security breaches which subsequently come to light. Those that try to cover up breaches which we subsequently become aware of are likely to face tougher regulatory sanctions.”

Who'd have thought that the woman who put a cat in a wheelie bin or the student who threw the fire extinguisher off Millbank Towers would ever be identified... ..but they were.

It is much more difficult to remain anonymous in today's information rich society. If a data controller leaks data into the public domain the public will enjoy reporting the breach to the Commissioner. - See the Hertfordshire case.

The Commissioner's press release of January 2010 says 262 breaches out of 800 were the result of theft, often where the personal information was held on an unencrypted portable device.

Prophetic words.

4 fines in 12 weeks around the end of 2010. At this rate and at the current level of fines there will be about 20 a year and £1,000,000 in total. How do organisations avoid this sort of sanction?

By using some common sense and putting in place training, policy and compliance with the Act. Once you are on the Commissioner's radar (whether you self report or a member of the public turns you in) you can expect not just a simple breach of principle 7 but a more

detailed look at your processing habits. There are after all seven more principles to breach.

And his power to audit the public sector without an invitation is being flexed as we word process. Who do you think might get the first such audit?

Paul Simpkins is a director of Act Now Training (www.actnow.org.uk). He is the course director for Act Now's ISEB Certificate in Data Protection course and runs the DP helpline.



The ISEB CERTIFICATE IN FREEDOM OF INFORMATION and ISEB CERTIFICATE IN DATA PROTECTION are ideal for those who wish to have their knowledge and expertise recognised through a formal qualification. The courses are designed in such a way as to allow those with a basic knowledge of DP and FOI to benefit and take the exam. Both courses are also accredited by the Solicitors Regulation Authority and the Institute of Legal Executives.

OUR GUARANTEE: If you attend the entire course (all days) and do not pass the exam, you may attend day 6 (mock exam and revision) and day 7 (revision and exam) again at another Act Now ISEB course for FREE. (The exam fee is still payable to ISEB).

For more details about our ISEB courses please visit: <http://www.actnow.org.uk/content/29>