Press release

24 November 2010

First monetary penalties served for serious data protection breaches

The Information Commissioner today served two organisations with the first monetary penalties for serious breaches of the Data Protection Act.

The first penalty, of £100,000, was issued to Hertfordshire County Council for two serious incidents where council employees faxed highly sensitive personal information to the wrong recipients. The first case, involving child sexual abuse, was before the courts, and the second involved details of care proceedings.

The second monetary penalty, of £60,000, was issued to employment services company A4e for the loss of an unencrypted laptop which contained personal information relating to 24,000 people who had used community legal advice centres in Hull and Leicester.

The Hertfordshire County Council breaches occurred in June 2010 when employees in the council's 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).

The first misdirected fax was meant for barristers' chambers and was sent to a member of the public. The council subsequently obtained a court injunction prohibiting any disclosure of the facts of the court case or circumstances of the data breach.

The second misdirected fax, sent 13 days later by another member of the council's childcare litigation unit, contained information relating to the care proceedings of three children, the previous convictions of two individuals, domestic violence records and care professionals' opinions. The fax was mistakenly sent to barristers' chambers unconnected with the case. The intended recipient was Watford County Court.

The Commissioner ruled that a monetary penalty of £100,000 was appropriate, given that the Council's procedures failed to stop two serious breaches taking place where access to the data could have caused substantial damage and distress. After the first breach occurred, the council did not take sufficient steps to reduce the likelihood of another breach occurring.

The A4e data breach also occurred in June 2010 following the company issuing an unencrypted laptop to an employee for the purposes of working at home. The laptop contained sensitive personal information when it was stolen from the employee's house.

The laptop contained personal information relating to 24,000 people who had used community legal advice centres in Hull and Leicester. An unsuccessful attempt to access the data was made shortly after the laptop was stolen. Personal details recorded on the system included full names, dates of birth, postcodes, employment status, income level, information about alleged criminal activity and whether an individual had been a victim of violence.

A4e reported the incident to the ICO. The company subsequently notified the people whose data could have been accessed.

The Commissioner ruled that a monetary penalty of £60,000 was appropriate, given that access to the data could have caused substantial

distress. A4e also did not take reasonable steps to avoid the loss of the data when it issued the employee with an unencrypted laptop, despite knowing the amount and type of data that would be processed on it.

Information Commissioner, Christopher Graham, said:

"It is difficult to imagine information more sensitive than that relating to a child sex abuse case. I am concerned at this breach – not least because the local authority allowed it to happen twice within two weeks. The laptop theft, while less shocking, also warranted nothing less than a monetary penalty as thousands of people's privacy was potentially compromised by the company's failure to take the simple step of encrypting the data".

"These first monetary penalties send a strong message to all organisations handling personal information. Get it wrong and you do substantial harm to individuals and the reputation of your business. You could also be fined up to half a million pounds."

ENDS

If you need more information, please contact the ICO press office on 0303 123 9070 or visit the website at: www.ico.gov.uk

Notes to Editors

1. The monetary penalty for Hertfordshire County Council is available on the ICO website here: http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Notices/hertfordshire_cc_monetary_penalty_notice.ashx
2. The monetary penalty for A4e is available on the ICO website here: http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Notices/a4e_monetary_penalty_notice.ashx
3. Monetary penalties are listed on the ICO website here: http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/taking_action.aspx
4. The Information Commissioner's Office upholds information rights in the public

interest, promoting openness by public bodies and data privacy for individuals.

5. The ICO has specific responsibilities set out in the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

6. For more information about the Information Commissioner's Office subscribe to our e-newsletter at www.ico.gov.uk. Alternatively, you can find us on Twitter at www.twitter.com/ICOnews.

7. Anyone who processes personal information must comply with eight principles, which make sure that personal information is:
    - Fairly and lawfully processed
    - Processed for limited purposes
    - Adequate, relevant and not excessive
    - Accurate and up to date
    - Not kept for longer than is necessary
    - Processed in line with your rights
    - Secure
    - Not transferred to other countries without adequate protection

8. The Data Protection Act (1998) does not cover the acts of interception of communications or 'hacking' of personal information. The interception of communications falls under the Regulation of Investigatory Powers Act (2000) which is regulated by the Interception of Communications Commissioner.

9. The ICO has legal powers to ensure that organisations comply with the requirements of the Data Protection Act. In using its regulatory powers, the ICO considers the nature and severity of the breach which has occurred. Dependent on circumstances, the powers the ICO has at its disposal include:
    - serving information notices requiring organisations to provide the ICO with specified information within a certain time period;
    - serving enforcement notices requiring organisations to take specified steps in order to ensure they comply with the law;
    - issuing monetary penalties of up to £500,000 for serious breaches of the Data Protection Act;
    - conducting audits to assess whether organisations are processing personal data in accordance with good practice;
    - reporting to Parliament on data protection issues of concern;
    - prosecuting those who commit criminal offences under the Act. The ICO prosecutes individuals and organisations for specific breaches of the Act such as the illegal trading of personal data and non-notification.