Data Protection Act 1998

Monetary Penalty Notice

Dated: 22 November 2010

Name: A4e Limited

Address: Bessemer Road, Sheffield S9 3XN

Statutory framework

---

1. A4e Limited is the data controller, as defined in section 1(1) of the Data Protection Act 1998 (the "Act"), in respect of the processing of personal data carried on by A4e Limited and is referred to in this notice as the "data controller". Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which he is the data controller.

2. The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act"). By virtue of section 6(1) of the Act, the office of the Data Protection Registrar originally established by section 3(1) (a) of the 1984 Act became known as the Data Protection Commissioner. From 30 January 2001, by virtue of section 18(1) of the Freedom of Information Act 2000 the Data Protection Commissioner became known instead as the Information Commissioner (the "Commissioner").

3. Under sections 55A and 55B of the Act (introduced by the Criminal Justice and Immigration Act 2008 which came into force on 6 April 2010) the Commissioner may, in certain circumstances, where there has there been a serious contravention of section 4(4) of the Act, serve a monetary penalty notice on a data controller requiring the data controller to pay a monetary penalty of an amount determined by the Commissioner and specified in the notice but not exceeding £500,000. The Commissioner has issued Statutory Guidance under section 55C (1) of the Act about the issuing of monetary penalties which is published on the Commissioner's website. It should be read in conjunction with the Data Protection (Monetary Penalties and Notices) Regulations 2010 and the Data Protection (Monetary Penalties) Order 2010.

Power of Commissioner to impose a monetary penalty

(1) Under section 55A of the Act the Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that –

(a) there has been a serious contravention of section 4(4) of the Act by the data controller,

(b) the contravention was of a kind likely to cause substantial damage or substantial distress, and

(c) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the data controller –

(a) knew or ought to have known –

(i) that there was a risk that the contravention would occur, and

(ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but

(b) failed to take reasonable steps to prevent the contravention.

Background

1. The data controller is contracted by the Legal Services Commission to operate the Community Legal Advice Centres in Hull and Leicester. The data controller also has other contracts with public sector organisations. Under the contractual arrangements the data controller is obliged to provide the Legal Services Commission and each of the two local authorities with monthly, quarterly and annual reports giving various statistics and certain other data specified in the contract.

2. The data controller employs approximately 3,250 staff and around 1,000 of those staff either work from home or otherwise remotely. One of the data controller's employees was working on these reports at

home. The data controller issued her with a laptop computer which did not contain any personal data but with the knowledge that it would be used for home working. The employee then loaded personal data and some sensitive personal data onto the laptop from the central secure servers. The only security on the laptop computer was password protection.

3. On the night of 18/19 June 2010 the employee was burgled at home with the loss of a number of possessions including the laptop computer holding the data controller's client data. The laptop computer was left on the table in the employee's dining room which was used as a home office. The burglary was reported to the data controller's IT department on discovery, in the early hours of 19 June 2010, and the user's account on the main server was immediately blocked.

4. Analysis of the system log files subsequently revealed that the employee's last authorised login had been at 16.04 on 18 June 2010, and there had been an unauthorised attempt to login at 22.36 on 18 June 2020 which was around the time of the burglary. It is possible that the burglar was attempting to access the laptop at that time, albeit unsuccessfully. The laptop computer has not been recovered.

5. The laptop computer held personal data and 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. Some of the data such as the data subject's ethnicity, disability status, employment status, income level and housing tenure was coded, although the codes were explained in a key which was also stored on the laptop computer in a separate Word document.

6. The data controller had commenced a prioritised programme of work in March 2009 to roll out encryption and port control across the IT estate that began with areas of service delivery where encryption was a contractual requirement and where access to personal data by front-line delivery staff led to an assessment of particular machines as high risk. The laptop computer issued to the employee formed part of the risk assessment but encryption of this laptop was scheduled for a later date of the phased roll out. This decision was made even though the data controller was contractually obliged to include, amongst other things, the client's name, date of birth and postcode in the reports referred to in paragraph 1 above. The first phase of encryption and port control lock down was completed in January 2010. This was followed by a second phase roll out to the remainder of the business as

soon as reasonably practicable.

7. There is no record of the employee undergoing any relevant induction training although the data controller states that the employee was issued with the relevant policies including the ICT governance policy, the cryptography policy and the security policy for laptop users when she joined the organisation. These policies contained instructions, amongst other things, that data (particularly sensitive data) should be kept to a minimum on local drives due to the risk of equipment theft; and that where possible no data should be stored on local PCs or laptops; and that any data that is temporarily stored on local machines must be encrypted. The security policy for laptop users also stated that when the laptop is not being used it should be locked away. According to the data controller its employees were also sent an email in early March 2010 reiterating the importance of data security and reminding them of its policies relating to laptop usage, encryption and port control, although no evidence of this email has been provided.

8. All of the data subjects affected by the security breach were informed by letter dated 29 June 2010. The Commissioner's office has received one formal complaint as a result of this security breach and, to date the data controller has received approximately 15 written communications from data subjects, three of whom initially suggested that they intended to pursue a claim for compensation against the data controller although no such claims have yet materialised. In addition, the data controller was contacted by approximately 3,200 data subjects either via the freephone helpline set up by the data controller on 30 June 2010 or in person. The data controller has stated that the vast majority of these data subjects were satisfied with the remedial action which had been taken.

9. The remedial action now taken by the data controller includes the development of compulsory information security training; the data controller's employees have also been sent a copy of the current ICT Code of Conduct requiring them to confirm by email that they are working in accordance with its requirements. In addition, encryption and port control has been rolled out to all personal computers and laptops used by the data controller to comply with its contractual obligations to the Legal Services Commission. Roll out to the rest of the data controller's portable computer stock has now been completed.

Grounds on which the Commissioner proposes to serve a monetary penalty notice

---

The relevant provision of the Act is the Seventh Data Protection Principle which provides, at Part I of Schedule 1 to the Act, that:

"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".

Paragraph 9 at Part II of Schedule 1 to the Act further provides that:

"Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to -

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

(b) the nature of the data to be protected".

- The Commissioner is satisfied that there has been a serious contravention of section 4(4) of the Act in that there has been a breach of the data controller's duty to comply with the Seventh Data Protection Principle in relation to all personal data with respect to which he is the data controller.

  In particular the data controller has failed to take appropriate technical and organisational measures against the accidental loss of personal data held on the laptop computer such as encrypting the laptop computer and providing the employee with security devices for the laptop computer for example, a Kensington lock or a cable. The Commissioner considers that the contravention is serious because the measures did not ensure a level of security appropriate to the harm that might result from such accidental loss and the nature of the data to be protected.

- The Commissioner is satisfied that the contravention is of a kind likely to cause substantial damage or substantial distress. The data controller's failure to take appropriate technical and organisational measures is likely to cause substantial damage and/or substantial distress to data subjects whose personal data and sensitive personal data may be disclosed to third parties.

  In this particular case the data subjects have suffered from substantial distress knowing that their personal data and sensitive personal data may be disclosed to third parties even though, as far as the

Commissioner is aware, those concerns have not so far materialised. This is evidenced by the number of complaints and other contacts the data controller received from data subjects. The data subject who complained to the Commissioner's office was also very distressed and anxious about her personal data being lost. This was aggravated by the fact that an unauthorised but unsuccessful attempt has already been made to access the data on the laptop computer which has still not been recovered. If the data is in fact disclosed to untrustworthy third parties then it is likely that the contravention would cause further distress and also substantial damage to the data subjects such as exposing them to identity fraud or causing damage to their personal reputations.

- The Commissioner is satisfied that section 55A (3) of the Act applies in that 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.

  The Commissioner has taken this view because the data controller issued the employee with a laptop computer with the knowledge that it would be used for home working and would have been aware from the start of the amount and nature of the personal data she would be processing on the laptop. The data controller should have encrypted the laptop computer before it was issued to the employee rather than leave it to the employee to arrange encryption. Despite the data controller's representations to the contrary, the Commissioner is satisfied that the data controller was aware that not all remote workers had access to the central secure network and that some were storing data locally. The data controller's action plan following the incident stated that not all remote workers have Net Extender installed and that VPN access speed is limited resulting in locally stored data. Although the employee may have been acting in breach of some of the data controller's policies, the data controller must have known about the problems that home workers were experiencing and that in practice the employee would have to load personal data onto her laptop computer in the absence of remote access.

  The data controller issued the unencrypted laptop despite being aware of the risks of failing to take appropriate technical and organisational measures against the accidental loss of personal data. At the time of the loss the data controller had a policy which required, amongst other things, that any data temporarily stored on a laptop computer must be encrypted. In addition the data controller had commenced a prioritised programme of work in March 2009 to roll out encryption which included

its laptop computers. It is regrettable that the laptop computer which was lost was not encrypted in the first phase of encryption and port control lock down which was commenced following the risk assessment carried out by the data controller and which ended in January 2010. However, the fact that the data controller had these policies and processes in place demonstrates that it recognised the risks of a security breach.

In the circumstances the data controller knew there was a risk that the contravention would occur unless reasonable steps were taken to prevent the contravention, such as encrypting the laptop computer, having sufficient remote access to the data on the data controller's central secure network for all remote workers, providing security devices for the laptop computer for example, a Kensington lock or a cable. In any event the data controller ought to have known that there was a risk that the contravention would occur unless the laptop computer was encrypted.

In view of the number of high profile data losses, the Commissioner's office provided published guidance on its website in November 2007 which clearly states that "There have been a number of reports recently of laptop computers, containing personal information which have been stolen from vehicles, dwellings or left in inappropriate places without being protected adequately. The Information Commissioner has formed the view that in future, where such losses occur and where encryption software has not been used to protect data, enforcement action will be pursued".

Further it should have been obvious to the data controller, which was routinely involved in handling large amounts of personal data that such a contravention would be of a kind likely to cause substantial damage or substantial distress to the data subjects due to the nature of the data involved. Although some of the sensitive personal data was coded, the decode key was held on the same laptop computer, albeit in a separate document, so it is possible that an unauthorised third party could still access this data and may already have done so.

Aggravating features the Commissioner has taken into account in determining the amount of a monetary penalty

---

Nature of the contravention

- Risk assessment carried out but stolen laptop computer still not encrypted

- No security devices provided to home workers
- The decode key to some of the sensitive personal data was held on the same laptop computer
- Unauthorised attempt made to access the data and laptop computer has not been recovered
- Contravention was particularly serious because of the sensitive nature of some of the personal data

Effect of the contravention

- The contravention was of a kind likely to cause substantial damage and substantial distress to the data subjects
- Large amount of sensitive data and personal data held on the laptop computer affecting 24,000 data subjects
- 15 written communications and contact from 3,200 data subjects

Behavioural issues

- The laptop computer was not encrypted despite employee working at home without remote access to the central secure server
- The laptop computer was only password protected
- Contravention was due to the negligent behaviour of the data controller in failing to take appropriate technical and organisational measures against the accidental loss of personal data

Impact on the data controller

- Sufficient financial resources to pay a monetary penalty up to the maximum without causing undue financial hardship

Mitigating features the Commissioner has taken into account in determining the amount of the monetary penalty

---

Nature of the contravention

- No previous similar security breach that the Commissioner is aware of
- Risk assessment was carried out
- Loss of laptop computer was reported within four hours and internal investigation began the same day
- Contravention was exacerbated by some actions of employee

Effect of the contravention

- Data is unlikely to be sufficient on its own to be used for fraudulent purposes

Behavioural issues

- Voluntarily reported to Commissioner's office
- Data controller fully cooperative with Commissioner's office
- The data controller wrote to all of the data subjects affected by the security breach and set up a freephone helpline to provide advice
- Data controller had started to roll out a programme of encryption and port control
- Substantial remedial action has now been taken

Impact on the data controller

- Significant impact on reputation of data controller as a result of these security breaches which could lead to a loss of business including its contracts with other public sector organisations

Other considerations

- The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the Act and this is an opportunity to reinforce the need for data controllers to ensure that appropriate and effective security measures, such as encryption, are applied to personal data held on laptop computers
- This will be one of the first monetary penalty notices issued by the Commissioner and is likely to set a precedent by which future notices will be judged

Notice of Intent

A Notice of Intent was served on the data controller dated 28 September 2010. The Commissioner received representations from the data controller in an undated letter from the Group Finance Director. The Commissioner has considered the written representations made in relation to the notice of intent when deciding whether to serve a monetary penalty notice. In particular, the Commissioner has taken the following steps:

- reconsidered the amount of the monetary penalty generally, and whether it is a reasonable and proportionate means of achieving the objective which the Commissioner seeks to achieve by this imposition;
- ensured that the monetary penalty is within the prescribed limit of £500,000; and
- ensured that the Commissioner is not, by imposing a monetary penalty, acting inconsistently with any of his statutory or public law duties and that a monetary penalty notice will not impose undue financial hardship on an otherwise responsible data controller.

Amount of the monetary penalty

The Commissioner considers that the contravention of section 4(4) of the Act is serious and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of £60,000 (Sixty thousand pounds) is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

Payment

The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 22 December 2010 at the latest. The monetary penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

Early payment discount

If the Commissioner receives full payment of the monetary penalty by 21 December 2010 the Commissioner will reduce the monetary penalty by 20% to £48,000 (forty eight thousand pounds).

Right of Appeal

There is a right of appeal to the (First-tier Tribunal) General Regulatory Chamber against:

a. the imposition of the monetary penalty

and/or;

b. the amount of the penalty specified in the monetary penalty notice.

Any Notice of Appeal should be served on the Tribunal by 5pm on 21 December 2010 at the latest. If the notice of appeal is served late the Tribunal will not accept it unless the Tribunal has extended the time for complying with this rule.

Information about appeals is set out in the attached Annex 1.

Enforcement

The Commissioner will not take action to enforce a monetary penalty unless:

- the period specified in the notice within which a monetary penalty must be paid has expired and all or any of the monetary penalty has not been paid;

- all relevant appeals against the monetary penalty notice and any variation of it have either been decided or withdrawn; and

- the period for the data controller to appeal against the monetary penalty and any variation of it has expired.

In England, Wales and Northern Ireland, the monetary penalty is recoverable by Order of the County Court or the High Court. In Scotland, the monetary penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court or any sheriffdom in Scotland.

Dated the 22nd day of November 2010

Signed: ……..

Christopher Graham
Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5A

ANNEX 1

SECTION 55 A-E OF THE DATA PROTECTION ACT 1998

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 48 of the Data Protection Act 1998 gives any person upon whom a monetary penalty notice or variation notice has been served a right of appeal to the (First-tier Tribunal) General Regulatory Chamber (the "Tribunal") against the notice.

2. If you decide to appeal and if the Tribunal considers:-

   a) that the notice against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

   the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

   GRC & GRP Tribunals
   PO Box 9300
   Arnhem House
   31 Waterloo Way
   Leicester
   LE1 8DJ

   a) The notice of appeal should be served on the Tribunal by 5pm on 21 December 2010 at the latest.

   b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

a) your name and address/name and address of your representative (if any);

b) an address where documents may be sent or delivered to you;

c) the name and address of the Information Commissioner;

d) details of the decision to which the proceedings relate;

e) the result that you are seeking;

f) the grounds on which you rely;

d) you must provide with the notice of appeal a copy of the monetary penalty notice or variation notice;

e) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 48 and 49 of, and Schedule 6 to, the Data Protection Act 1998, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).