

Data Protection Act 1998

Monetary Penalty Notice

Dated: 13 September 2012

Name: Chief Constable of Greater Manchester Police

**Address: Chester House, PO Box 22, Boyer Street, Manchester M16
ORE**

Statutory framework

1. The Chief Constable of Greater Manchester Police 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 out by Greater Manchester Police 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 it 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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)


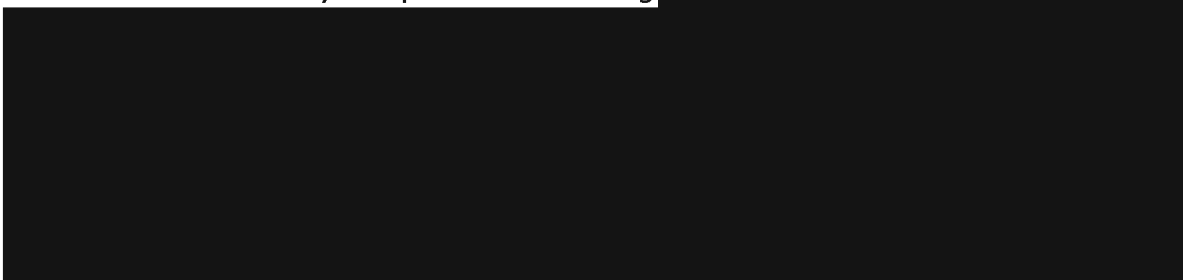
Regulations 2010 and the Data Protection (Monetary Penalties) Order 2010.

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

4. On 17 July 2011, an officer employed by the data controller had his house burgled resulting in the theft of (among other things) a personal USB stick which he kept in his wallet. The USB stick was unencrypted and had no password protection. At the time of the burglary, the officer had left the wallet (which contained the USB stick, cash and cards) on the kitchen table next to his car keys. None of the items stolen in the burglary (including the USB stick) have been recovered to date.

5. The officer had worked in the data controller's Serious Crime Division (mainly the Drug Squad) for a period of approximately 10 years. During this period the officer used a personal USB stick to download information from his folder on the shared drive of the data controller's network which was subject to access controls. The information was downloaded to create a backup of his folder and to enable the officer to access information when he was out of the office or at another site. The officer had been issued with an unencrypted USB stick by the data controller in 2003/2004 but he replaced it himself when the memory was full with a USB stick with larger capacity. At the time of the security breach a significant number of officers across the Force were routinely using such devices although the Commissioner accepts that they were not necessarily storing sensitive personal data.
6. Following a forensic investigation of the officer's computer by the data controller it was discovered that the USB stick contained the personal data (some of which was sensitive) of approximately 1,075 individuals stored over an 11-year period including 

7. The data controller regularly issues Chief Constable's Orders ("CCO") which can cover any aspect of the working environment. CCO 2010/38 was issued in September 2010 and ordered all staff to use encrypted USB sticks issued by the data controller. However, the Commissioner understands both that this officer was on leave at the time this CCO was issued and that he had never had any specific training on data protection. After the CCO was issued by the data controller it was not effectively enforced and no further steps were taken to prevent the use of USB sticks other than encrypted ones issued by the data controller.
8. Following the security breach the data controller held an amnesty to recover any personal and/or unencrypted devices. This resulted in the recovery of approximately 1,100 such USB sticks, although it is possible that some of the devices have still not been recovered. The data controller has now taken additional remedial action by implementing endpoint security which prevents any download of information to unauthorised USB devices.

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 particular, the data controller has failed to take appropriate technical and organisational measures against the accidental loss of personal data such as a combination of training staff on the importance of using encrypted USB sticks; effective management controls; and limiting access to the data controller's network. The Commissioner considers that the contravention is serious because the measures did not ensure a level of security appropriate to the nature of the data to be protected and the harm that might result from accidental loss.

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

In this particular case, the data subjects would suffer from substantial distress knowing that their sensitive personal data may be disclosed to third parties even though, so far as the Commissioner is aware, those concerns have not so far materialised. This is aggravated by the fact that the USB stick has still not been recovered.

If the data has in fact been accessed by untrustworthy third parties then it is likely that the contravention would cause further distress and substantial damage to the data subjects such as exposing them to physical harm.

- 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 and/or substantial distress, but failed to take reasonable steps to prevent the contravention.

The Commissioner has taken this view because officers across the Force were routinely downloading information from the network and the data controller would have been aware of the sensitive nature of the personal data they were storing on USB sticks. Further, as a result of a similar security breach in September 2010 the data controller had made the decision to issue CCO 2010/38.

In the circumstances, the data controller knew or ought to have known that there was a risk that the contravention would occur unless reasonable steps were taken to prevent the contravention such as a combination of training staff on the importance of using encrypted USB sticks; effective management controls; and limiting access to the data controller's network.

Further, it should have been obvious to the data controller whose officers were routinely involved in handling large amounts of sensitive personal data, that such a contravention would be of a kind likely to cause substantial damage and/or substantial distress to the data subjects due to the nature of the data involved. It is possible that an unauthorised third party could still obtain 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

- A similar security breach occurred in September 2010 albeit involving no sensitive personal data
- Contravention was particularly serious because of the sensitive nature of the personal data involved in the security breach

- The data related to approximately 1,075 data subjects over an 11 year period

Effect of the contravention

- USB stick has still not been recovered
- Some of the data subjects could be at significant risk if the information on the USB stick was disclosed to untrustworthy third parties
- The contravention was of a kind likely to cause substantial damage and/or substantial distress to the data subjects

Behavioural issues

- Data controller failed to take sufficient remedial action following the previous security breach to prevent a recurrence

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

- CCO issued in September 2010 ordering all staff to use encrypted USB sticks

Effect of the contravention

- No evidence to suggest that the personal data has been inappropriately processed

Behavioural issues

- Voluntarily reported to the Commissioner's office
- Data controller fully co-operative with Commissioner's office
- Data controller conducted risk assessment and informed the data subjects most at risk about the security breach
- Full investigation carried out
- Some remedial action has now been taken

Impact on the data controller

- Liability to pay monetary penalty will fall on the public purse although the penalty will be paid into the Consolidated Fund
- Significant impact on reputation of data controller although the security breach has already received local media coverage

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 are applied to personal data

Notice of Intent

A notice of intent was served on the data controller dated 12 July 2012. The Commissioner received written representations from the data controller in a letter dated 17 August 2012. 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 very serious and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of £150,000 (One hundred and fifty 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 16 October 2012 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 15 October 2012 the Commissioner will reduce the monetary penalty by 20% to £120,000 (One hundred and twenty 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 15 October 2012 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 13th day of September 2012

Signed:

David Smith
Deputy Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

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 15 October 2012 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)).