

Data Protection Act 1998

Monetary Penalty Notice

Dated: 24 September 2013

Name: Jala Transport Limited

Address: 782, Harrow Road, Wembley, Middlesex HA0 3EL

Statutory framework

1. Jala Transport 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 out by Jala Transport 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 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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. The data controller is a small money lending business that, at the time of the breach, was regulated by the Financial Services Authority. On 3 August 2012, the data controller's sole proprietor was driving to work and had stopped at a junction. A thief reached in through an open window and stole his briefcase from a seat in the car. The briefcase contained an external hard drive, some documents and approximately £3,600 in cash.
5. The external hard drive was protected by an 11-character (letters and numbers) password, but it was unencrypted. It contained a complete copy of the data controller's customer database including the details of approximately 250 clients such as their name, address, contact number, date of birth, nationality, passport number, proof of address

(utility bills and bank statements) and proof of identity (passports and driving licences).

6. The Commissioner understands that the stolen external hard drive contained the only copy of the data controller's customer database and that it was taken home at the end of each working day for business continuity purposes and to reduce the risk of damage or theft. The external hard drive has still not been recovered.

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".

In deciding to issue this Monetary Penalty Notice, the Commissioner has considered the facts of the case and the deliberations of those within his office who have recommended this course of action. In particular, he has considered whether the criteria for the imposition of a monetary penalty have been met; whether, given the particular circumstances of this case and the underlying objective in imposing a monetary penalty, the imposition of such a penalty is justified; and whether the amount of the proposed penalty is proportionate.

- The Commissioner is satisfied that there has been a serious contravention of the seventh data protection principle.

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 encrypting the external hard drive containing the back-up data, closing the car window and placing the briefcase in the boot of his car or out of sight.

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 such 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 personal data may be disclosed to third parties who have no right to see that information.

In this particular case, the data subjects would suffer from substantial distress knowing that their personal data may be disclosed to unauthorised 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 external hard drive 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 identity fraud and possible financial loss.

- 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 a large amount of personal data relating to the data controller's customers was held on the external hard drive. The data controller was used to dealing with such information on a daily basis and had therefore taken some steps to safeguard the information on the external hard drive by having it password protected and taking the customer database home at the end of each working day to reduce the risk of damage or theft.

In view of the number of high profile data losses, the Commissioner's office 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”.

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 encrypting the external hard drive containing the back-up data, closing the car window and placing the briefcase in the boot of his car or out of sight.

Further it should have been obvious to the data controller who 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 the external hard drive was password protected 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

Effect of the contravention

- External hard drive has still not been recovered

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

Effect of the contravention

- External hard drive was password protected
- No evidence to suggest that the personal data has been inappropriately processed
- No complaints received from the data subjects to date

Behavioural issues

- Voluntarily reported to the Commissioner’s office
- Data controller co-operative with Commissioner’s office

- Remedial action has now been taken

Impact on the data controller

- Significant impact on reputation of data controller

Other considerations

- The Third Data Protection Principle at Part I of Schedule 1 to the Act was also contravened because the data controller did not retain a copy of the customer database that was stolen
- 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 small and medium sized 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 1 August 2013. The Commissioner has not received any written representations from the data controller in response to the notice of intent. In the circumstances, the Commissioner has now 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 the seventh data protection principle is serious and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of £5,000 (Five thousand pounds) is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

In reaching this decision, the Commissioner considered other cases of a

similar nature in which a monetary penalty has been imposed and the facts and aggravating and mitigating features referred to above. Of particular relevance in this case is the nature of the personal data that has been put at risk despite a number of high profile data losses of a similar nature that should have prompted the data controller to encrypt the hard drive.

Payment

The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 1 November 2013 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 31 October 2013 the Commissioner will reduce the monetary penalty by 20% to £4,000 (Four 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 31 October 2013 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 24th day of September 2013

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 31 October 2013 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)).