

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

ENFORCEMENT NOTICE DATED 14 JULY 2008

To: The Chairman

of: HM Revenue and Customs
100 Parliament Street
London
SW1A 2BQ

1. The Commissioner's of HM Revenue and Customs ("HMRC") 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 by HMRC and is referred to in this notice as 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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. The Commissioner was informed of an incident involving the loss of two compact discs holding the personal data of up to 25 million individuals. The circumstances were that on 18 October 2007 both compact discs were sent by the Child Benefit Office in Washington, Tyne and Wear to the National Audit Office ("NAO") in London via the data controller's internal post system which is operated by a courier company. The data was being sent to the NAO in response to a request for information for audit purposes. The package containing the data was not recorded or registered, the compact discs were lost and no trace of them has been found.
4. In response Kieran Poynter of PricewaterhouseCoopers was commissioned by the Chancellor of the Exchequer to carry out a review resulting in the Poynter Report dated 25 June 2008 (the "Poynter Report"). The terms of reference were, amongst other things, "To establish the circumstances that led to the significant loss of confidential personal data on Child Benefit recipients and other recent losses of confidential data and the lessons to be learnt, and the light of those circumstances to examine HMRC practices and procedures in the handling and transfer of confidential data on taxpayers and benefit/credit recipients; the processes for ensuring that these procedures are communicated to staff and the safeguards in place to ensure they are adhered to; the reasons why these failed to prevent the loss of confidential data; whether these procedures and processes are sufficient to ensure the confidentiality of personal data".

5. The Commissioner has considered the Poynter Report which makes 45 Recommendations at section XIV of the said report. The Commissioner has also been provided with a copy of the independent investigation report into loss of data relating to Child Benefit by the Independent Police Complaints Commission (“IPCC”). The IPCC report was focused on the data loss as a public protection issue and to investigate the circumstances of the disappearance of the personal data and by doing so identify its current location in order to reduce potential harm. The Commissioner has further considered the data controller’s compliance with the provisions of the Act in light of these matters.
6. In particular the Commissioner has taken into account the fact that the lost compact discs held personal data for up to 25 million individuals and that the data loss was avoidable. The Poynter Report also found that the personal data had been provided to the NAO in full, even though the NAO had only requested a large sample of the data and had attempted to get some of the information redacted, albeit primarily to reduce the size of the data file. In the circumstances the missing compact discs held an excessive amount of personal data. The Commissioner has also had regard to the fact that the lost compact discs were password protected but not encrypted at the time they went missing.
7. 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 with respect to which he is the data controller. The relevant provisions of the Act are the Third and Seventh Data Protection Principles.
8. The Third Data Protection Principle provides, at Part 1 of Schedule 1 to the Act that:

“Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed”.
9. The Seventh Data Protection Principle provides at Part 1 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 of Part II of Schedule 1 of 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”.

10. Having considered the report referred to in paragraph 4 above together with the IPCC report, the Commissioner is satisfied that the data controller has contravened the Third Data Protection Principle in that the personal data processed on the missing compact discs were excessive for the purpose for which they were processed. Moreover, the Commissioner is also satisfied that the data controller has contravened the Seventh Data Protection Principle in that he failed to take appropriate measures to ensure the security of its data.
11. The Commissioner considered, as he is required to do under Section 40(2) of the Act when deciding whether to serve an Enforcement Notice, whether any contravention has caused or is likely to cause any person damage or distress. The Commissioner took the view that the likelihood of distress is self-evident: the 25 million or so individuals whose data has been lost are likely to have suffered worry and anxiety on account of the risk that their data will come into the possession of unauthorised individuals. In reaching this view the Commissioner has had regard to the measures put in place to safeguard the data and to reassure the public.
12. The Commissioner has further taken account of the effect of the incorporation in English law of the European Convention on Human Rights (“ECHR”), by virtue of the Human Rights Act 1998, in deciding whether or not to serve an Enforcement Notice. In particular, the Commissioner is mindful of the provisions of Article 8 of the ECHR in that the individuals whose personal data was held on the missing compact discs all have the right to respect for private and family life, home and correspondence.

In view of the matters referred to above the Commissioner hereby gives notice that, in exercise of his powers under section 40 of the Act, the data controller is required to take the following specified steps to comply with the Third and Seventh Data Protection Principles.

The data controller, HM Revenue and Customs, shall:

- (1) use its best endeavours to give effect to the Recommendations still to be implemented in section XIV of the Poynter Report within 36 months of the date of the said Report.
- (2) Provide the Commissioner with progress reports through its Data Security Programme after 12, 24 and 36 months of the 31 July 2008 documenting in detail how the Recommendations of the Poynter Report have been, or are being, implemented.

Right of Appeal

There is a right of appeal against this Notice to the Information Tribunal. Information about appeals is set out in the attached Annex 1.

Any Notice of Appeal should be served on the Tribunal within 28 days of the date on which this Notice is served. If the notice of appeal is served late the Tribunal will not accept it unless it is of the opinion that it is just and right to do so by reason of special circumstances.

Dated the 14th day of July 2008

Signed:

Richard Thomas
Information Commissioner
Wycliffe House
Water Lane
WILMSLOW
Cheshire
SK9 5AF

ANNEX 1

THE DATA PROTECTION ACT 1998 (PART V, SECTION 40)

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 48 of the Data Protection Act 1998 gives any person upon whom an enforcement notice or an information notice has been served a right of appeal to the Information Tribunal (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 Secretary to the Information Tribunal, Arnhem House Support Centre, PO Box 6987, Leicester, Leicestershire, LE1 6ZX.
 - a) The notice of appeal should be served on the Tribunal within 28 days of the date on which notice of the Commissioner's decision was served on or given to you.
 - b) If your notice of appeal is late the Tribunal will not accept it unless it is of the opinion that it is just and right to do so by reason of special circumstances.
 - c) If you send your notice of appeal by post to the Tribunal, either in a registered letter or by the recorded delivery service, it will be treated as having been served on the Tribunal on the date on which it is received for dispatch by the Post Office.
4. The notice of appeal should state:-
 - a) your name and address;
 - b) the decision which you are disputing and the date on which the notice relating to such decision was served on or given to you;
 - c) the grounds of your appeal;
 - d) whether you consider that you are likely to wish a hearing to be held by

the Tribunal or not;

e) if you have exceeded the 28 day time limit mentioned above the special circumstances which you consider justify the acceptance of your notice of appeal by the Tribunal; and

f) an address for service of notices and other documents on you.

In addition, a notice of appeal may include a request for an early hearing of the appeal and the reasons for that request.

5. By virtue of section 40(7), an enforcement notice may not require any of the provisions of the notice to be complied with before the end of the period in which an appeal can be brought and, if such an appeal is brought, the notice need not be complied with pending the determination or withdrawal of the appeal.

However, section 40(7) does not apply where the notice contains a statement that the Commissioner considers that the notice should be complied with as a matter of urgency.

Section 48(3) provides that where an enforcement notice contains a statement that the notice should be complied with as a matter of urgency then, whether or not you intend to appeal against the notice, you may appeal against -

(a) the Commissioner's decision to include the statement in the notice, or
(b) the effect of the inclusion of the statement as respects any part of the notice.

6. 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.
7. The statutory provisions concerning appeals to the Information Tribunal are contained in sections 48 and 49 of, the Schedule 6 to, the Data Protection Act 1998, and the Information Tribunal (Enforcement Appeals) Rules 2005 (Statutory Instrument 2005, No. 14).