

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

ENFORCEMENT NOTICE DATED 23 JANUARY 2008

To: Marks & Spencer PLC

of: Waterside House
35 North Wharf Road
London
W2 1NW

- 1 Marks & Spencer PLC ("M&S"), is a "data controller" as defined in Section 1(1) of the Data Protection Act 1998 (the "Act").
- 2 The Commissioner has considered a report that has been provided to him by [NAME REMOVED], Head of Data Protection on behalf of the data controller regarding the theft of a laptop computer holding personal data.
- 3 The data controller employed the services of an independent [NAME REMOVED] company ("the data processor") in connection with the preparation of personal pension change statements for members of the M&S pension scheme. To facilitate this, the data processor had access to personal data containing the membership of the M & S Pension Scheme. On 18 April 2007 a laptop computer holding this personal data was stolen during a burglary at the home of the Managing Director of the data processor. The personal data was held on the laptop computer because on 16 April 2007, in preparation for a meeting that day, the Managing Director of the data processor had taken the decision to download this data onto his laptop computer. The personal data related to approximately 26,000 M & S employees. The laptop computer was unencrypted.
- 4 The Commissioner has considered the report provided to him on the issues arising from the incident referred to in paragraph 3 above. The Commissioner has considered the data controller's compliance with the provisions of the Act in light of this matter.
- 5 Section 4(4) of the Act provides that, subject to Section 27(1), 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 Seventh Data Protection Principle, which states:

"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 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”*

Paragraph 11 of Part II of Schedule 1 of the Act provides that:

“Where processing of personal data is carried out by a data processor on behalf of the data controller, the data controller must.....

- (a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and*
- (b) take reasonable steps to ensure compliance with those measures*

- 6 Having considered the report referred to in paragraph 2 above, the Commissioner takes the view that in this case the personal data held on the laptop computer should have been encrypted so that in the event of its theft it would not have been possible to view the personal data in a readable format. The Commissioner has come to the view that the data controller’s processing contravenes the Seventh Data Protection Principle in that it failed to take appropriate measures to ensure the security of its data.
- 7 On 9 July 2007 the Commissioner served a Preliminary Enforcement Notice on M & S. This notice indicated that the Commissioner was minded to serve an Enforcement Notice requiring the data controller to take specified steps to comply with the Seventh Data Protection Principle. Representations have been received in the form of a number of letters from [NAME REMOVED], Solicitor acting on behalf of M & S.
- 8 The Commissioner has sought to resolve this matter by informal means. At an early stage in negotiations it was agreed that the Commissioner would be willing to accept undertakings concerning compliance with the Seventh Data Protection Principle as an alternative to issuing an Enforcement Notice. However M & S have concluded they are only prepared to provide undertakings on condition they are not made public which is not acceptable to the Commissioner.
- 9 The Commissioner has 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 takes the view that damage or distress is likely as a result of personal data getting into the hands of unauthorised persons.

10 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, he requires that the data controller shall take the following steps:

- **Ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Schedule 1 Part I of the Act and, in particular, ensure that the process of laptop hard drive encryption commenced by the data controller in October 2007 is completed by 1st April 2008**

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 23rd day of January 2008

Signed:

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