

DATA PROTECTION ACT 1998
SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER
ENFORCEMENT NOTICE
DATED: 4 June 2013

To: Glasgow City Council

of: City Chambers, Glasgow G2 1DU

1. Glasgow City Council 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 Glasgow City Council 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the '1984 Act').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 in which two unencrypted laptops, one of which contained a substantial amount of personal data, including bank account details, were stolen from offices of the data controller which were then under refurbishment. There had been previous thefts of equipment from these offices, but physical security measures had not been improved.
4. The Commissioner had served the data controller with an Enforcement Notice in 2010 following the loss of an unencrypted USB memory stick containing personal data, but noted that unencrypted laptops were still being issued to some employees over two years later. It was also noted during the investigation of this incident that over 70 other unencrypted laptops were unaccounted for – some or all of which may also have contained personal data; and it was further revealed that the data

controller's asset register was incomplete and contained inaccuracies.

5. The Commissioner has considered the data controller's compliance with the provisions of the Act in light of these matters. In particular, he has taken note of the remedial action already taken by the data controller.
6. 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 provision of the Act is the Seventh Data Protection Principle.
7. The Seventh Data Protection Principle 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 of 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."*

8. Having considered the facts of this case and the the remedial action already taken by the data controller , the Commissioner is satisfied that the data controller has contravened the Seventh Data Protection Principle in that it failed to take appropriate measures to ensure the security of its data.
9. 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 20,143 individuals whose personal data has been stolen 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 particular, the 6,069 individuals whose bank account details were included in the data stolen are likely to have suffered significant distress at the loss. While there is no evidence that damage has been caused, there was a significant risk that it could have been.

10. 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 laptops 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, he requires that the data controller shall:

- (1) Conduct a full audit of all existing IT assets used to process personal data by 30 June 2013;
- (2) Create a new asset register by 31 July 2013;
- (3) Carry out a full reconciliation every year thereafter to ensure that the asset register is up to date;
- (4) Provide training to managers in relation to asset management by 30 June 2013;
- (5) Re-issue the information security guidelines and update the information security training for 'All Staff' in relation to the data controller's policy on encrypting portable devices and removable media by 30 June 2013.

Right of Appeal

There is a right of appeal against this Notice to the First-tier Tribunal (Information Rights), part of the General Regulatory Chamber. 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 4th day of June 2013

Signed:

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