

30/11/09

**DATA PROTECTION ACT 1998
UNDERTAKING**

Data Controller: **Department of Finance and Personnel
Rathgael House
2nd Floor
Balloo Road
Bangor
Co Down BT19 7NA**

I, Stephen Peover, Permanent Secretary responsible for the Department of Finance and Personnel, for and on behalf of the Department hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Department of Finance and Personnel 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 the Department of Finance and Personnel and is referred to in this Undertakings 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 a data controller.
2. The Information Commissioner (the "Commissioner") was informed by the Department of Finance and Personnel about the theft of 12 laptop computers, 2 of which contained significant personal data.
3. The password protected laptop computers containing personal data relating to approximately 37000 individuals were either secured to desks or in locked cabinets. The computers contained payroll, employment and health information although not all records contained all these categories of information. Approximately 900 records contained bank details.
4. The Commissioner has considered the data controller's compliance with the provision of the Act in the light of this matter. The relevant provision of the Act is the Seventh Data Protection Principle. This Principle is set out in Schedule 1 Part 1 of the Act. The Commissioner has also considered the fact that some of the data stolen in this incident consisted of information defined as "sensitive personal data" under section 2 of the Act.

5. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

The data controller shall, as from date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part 1 of Schedule 1 to the Act, and in particular that:

- (1) Portable and mobile devices including laptops and other portable media used to store and transmit personal data, the loss of which could cause damage or distress to individuals, are encrypted using encryption software which meets the current standard or equivalent;
- (2) Physical security measures are adequate to prevent unauthorised access to personal data;
- (3) Staff are aware of the data controller's policy for the storage and use of personal data and are appropriately trained how to follow that policy;
- (4) The policy covering the storage and use of personal data is followed by staff;
- (5) The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Dated

30 / 11 / 2009

Signed

Stephen Peover

Department of Finance and Personnel

Signed

Mark Gorrill

Assistant Commissioner, Regulatory Action Division

For and on behalf of the Information Commissioner