

DATA PROTECTION ACT 1998

16/3/10

UNDERTAKING

Data Controller: The Royal London Mutual Insurance Society Ltd
55 Gracechurch Street
London
EC3V 0RL

I, Michael Yardley, Group Chief Executive Officer of The Royal London Mutual Insurance Society Ltd ("Royal London"), for and on behalf of Royal London, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Royal London 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 Royal London and is referred to in this Undertaking 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 provided with a report of the theft or loss of eight laptops from the Edinburgh offices of the data controller, which occurred sometime between 15 April and 15 June 2009. Two of the laptops were unencrypted, although they were password-protected. They contained a significant amount of personal data relating to 2,135 individuals. These individuals were employees of various firms which had sought pension scheme illustrations from the data controller via independent financial advisers.
3. The internal investigation revealed that the data controller was uncertain of the precise location of these laptops at any given time. Physical security measures in place at the most likely location were discovered to be inadequate. The internal report indicated that managers were unaware of the fact that any of the laptops contained any personal data, and thus did not take additional precautions to control and secure it. Upon discovery of the loss, physical security measures were enhanced and other remedial actions initiated.
4. The Commissioner has considered the data controller's compliance with the provisions 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 I to 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 the 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 I 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. In this respect, certain specific security controls agreed with the Commissioner's Office on 20 February 2009 will continue in operation;**
- (2) Appropriate physical security measures are taken to prevent unauthorised access to personal data;**
- (3) All staff are made 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 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.....16/03/2010.....

Signed....

Michael Yardley

Group Chief Executive Officer

The Royal London Mutual Insurance Society Ltd

Signed....

Mick Gorrill

Head of Enforcement

For and on behalf of the Information Commissioner