

Press Release

For immediate release

17 March 2010

Action taken after insurance provider loses over 2,000 people's details

The Information Commissioner's Office (ICO) has found that the Royal London Mutual Insurance Society breached the Data Protection Act (DPA) after eight laptops, two of which contained the personal details of 2,135 people, were stolen from the company's Edinburgh offices. The individuals affected were employees of various firms which had sought pension scheme illustrations.

The two laptops containing personal information were unencrypted but were password protected. An internal report established that the company was uncertain about the precise location of the laptops at any given time and that physical security measures were inadequate. The report also revealed that managers were not aware that personal information was stored on any of the laptops, which meant no additional precautions to control and secure the data had been taken.

Michael Yardley, Group Chief Executive Officer of the company, has now signed an official [Undertaking](#) to ensure that portable and mobile devices including laptops are encrypted. The Undertaking also requires appropriate physical security measures to be put in place to prevent unauthorised access to personal data. All staff will now be made aware of the company's policy for storage and use of personal data.

Mick Gorrill, Head of Enforcement at the ICO, said: "It is crucially important that portable devices such as laptops containing personal information are properly protected. It is particularly concerning that the organisation was unaware of the whereabouts of the laptops at any given time or what information they held. All staff members should be fully aware of the policies and procedures in place to safeguard personal information and should be appropriately trained. I am pleased the Royal London Mutual Insurance Society Ltd has agreed to take further remedial steps to prevent a similar incident happening again."

A full copy of the Undertaking can be viewed here:

http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx

ENDS

If you need more information, please contact the ICO press office on 020 7025 7580 or visit the website at: www.ico.gov.uk

Notes to Editors

1. 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.

2. The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

3. The ICO is an independent body with specific responsibilities set out in the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

4. For more information about the Information Commissioner's Office subscribe to our e-newsletter at www.ico.gov.uk. Alternatively, you can find us on Twitter at www.twitter.com/ICOnews

5. Anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection