

Press Release

For immediate release

24 March 2010

Zurich Insurance agrees to improve information security after losing over 46,000 individuals' personal financial information

The Information Commissioner's Office (ICO) has found Zurich Insurance plc in breach of the Data Protection Act after it lost an unencrypted back-up tape containing financial personal information belonging to 46,000 policy holders of Zurich Private Client, Zurich Special Risk and Zurich Business Client, which are all part of Zurich Insurance plc.

The back-up tape, which also included personal details of 1,800 third parties, was lost by a sister company, Zurich Insurance Company South Africa, during a routine transfer to a data storage centre in South Africa. The data loss occurred on 11 August 2008 although the sister company did not inform Zurich Insurance plc until over a year later. Subsequent internal investigations revealed failings in the management of security procedures involving data tapes in South Africa.

UK Branch Manager of Zurich Insurance plc, Stephen Lewis, has now signed an [Undertaking](#) to ensure that where any future movement of back-up tapes is required appropriate data security procedures including the use of encryption where appropriate, are in place. Zurich Insurance plc has committed to put in place controls to monitor and promptly report potential or actual data loss activity. The Undertaking also requires that steps are taken to ensure staff and external contractors are made fully

aware of security procedures and adequate checks are carried out on contractors' staff.

Sally-anne Poole, Head of Enforcement & Investigations at the ICO, said: "It is vital that organisations ensure effective safeguards are in place to protect personal information. Failure to adequately protect personal details could lead to information falling into the wrong hands and ultimately the loss of customers' trust and confidence. I encourage all organisations to report any serious data security breaches to us so that the nature of the breach or loss can be considered. I am pleased to see that Zurich Insurance plc has taken remedial steps to ensure individuals' personal details are protected in future."

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 1 of schedule 1 to the Act, and in particular that:
 - where any future movement of back up tapes is required ensure that appropriate data security procedures, including the use of encryption where appropriate, are in place;
 - steps are taken to ensure staff and external contractors are made fully aware of such security procedures and adhere to them;
 - adequate checks are carried out on contractors' staff;
 - and effective controls are put in place to monitor and promptly report potential or actual data loss activity.

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 has 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. Organisations can now sign the Personal Information Promise to demonstrate their commitment to protecting people's personal information by visiting the website at www.ico.gov.uk
5. 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
6. 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