

[REDACTED]

7/3/10

## DATA PROTECTION ACT 1998

### UNDERTAKING

Data Controller: Zurich Insurance plc

3000 Parkway  
Whiteley  
Fareham  
PO15 7JZ

I, Stephen Lewis, UK Branch Manager of Zurich Insurance plc, 3000 Parkway, Whiteley, Fareham, PO15 7JZ for and on behalf of Zurich Insurance plc hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Zurich Insurance plc 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 Zurich Insurance plc 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 initially informed of a self reported breach of data security by the data controller on 3 October 2009. After further investigations by the data controller a formal security breach notification was provided to the Commissioner on 27 January 2010.
3. The data loss occurred on 11 August 2008 during the transfer of personal data of some of the data controller's UK customers by its sister company, Zurich Insurance Company South Africa, for data processing purposes. An unencrypted back up tape was lost during a routine transfer to a data storage centre in South Africa. The back up tape included various financial personal data of 46,000 policy holders of Zurich Private Client, Zurich Special Risk and Zurich Business Insurance, which are part of the data controller and 1,800 third parties such as claimants. The data controller took steps to notify customers affected by the data loss in October 2009. Further investigations by the data controller revealed deficiencies in the management of security procedures involving data tapes in South Africa. As such, a further 5,000 of the data controller's UK customers whose personal data was not on the lost tape, but whose personal data was otherwise held in South Africa and who may have been potentially affected by the deficiencies, were notified.
4. The Commissioner has considered the data controller's compliance with the provisions of the Act in light of the matter. The relevant


provision of the Act is the Seventh Data Protection Principle. This Principle is set out in Schedule 1 Part 1 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 1 of schedule 1 to the Act, and in particular that:**

- (1) 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;**
- (2) steps are taken to ensure staff and external contractors are made fully aware of such security procedures and adhere to them;**
- (3) adequate checks are carried out on contractors' staff; and**
- (4) effective controls are put in place to monitor and promptly report potential or actual data loss activity.**

Dated..... 7/3/200

Signed   
For and on behalf of Zurich Insurance plc

Signed.....   
Mick Gorrill  
Assistant Commissioner Regulatory Action Division  
For and on behalf of the Information Commissioner