

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Jubilee Managing Agency Ltd

Sidcup House
12-18 Station Road
Sidcup
Kent
DA15 7EX

I, Kate Lewis, Managing Director of Jubilee Managing Agency Ltd, Sidcup House, 12-18 Station Road, Sidcup, Kent DA15 7EX ("the Company"), on behalf of the Company, hereby acknowledge the details set out below and confirm the Company's agreement to comply with the terms of the following Undertaking:

1. Jubilee Managing Agency Ltd 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 on by the Company and by several data processors 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 from the data controller's Compliance Director, regarding the loss of an unencrypted disk containing personal data, including financial information, relating to around 2100 individual UK policyholders. Some of the data related to policies that had expired or been cancelled, in some cases over 10 years ago, or to policyholders who had since died or moved address.
3. The data controller conducted a full investigation and subsequently commissioned a review of its data security arrangements by an independent company. That review highlighted several weaknesses to be addressed, including a lack of documentation of procedures and policies relating to data security and insufficient training of staff.
4. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provisions of the Act are the Fifth and Seventh Data Protection Principles. These are set out at Part I of Schedule 1 to the Act.
5. In view of the circumstances of this incident and the remedial steps taken by the data controller as a result, it has been 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 1 July 2009, and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data is processed in accordance with the Fifth and Seventh Data Protection Principles in Part I of Schedule 1 to the Act, and in particular that:

- 1. The data controller shall ensure that any personal data held on, or transferred by means of, any removable media, either by the data controller or by a data processor acting on the data controller's behalf, is suitably encrypted, or other technical and operational measures are taken offering a comparable level of security, so as to provide effective protection against unauthorised access;**
- 2. The data controller shall adopt detailed written procedures in relation to data protection, based on the data protection principles in the Act, to provide adequate and consistent advice for all staff on how to manage these aspects of their work and to allow for effective risk assessment and compliance monitoring, as recommended by the independent review;**
- 3. The data controller shall ensure that personal data is not kept for longer than necessary and that, when no longer needed, such data is securely erased;**
- 4. The data controller shall improve its training and awareness programme, making data protection training mandatory at induction, for its own staff and all temporary or contract staff, and shall refresh such training on a regular basis;**
- 5. Where processing of personal data is carried out by a data processor on behalf of the data controller, the data controller shall ensure that such processing is carried out in accordance with the seventh data protection principle, having due regard to the interpretive provisions set out in paragraphs 11 and 12 of Part II of Schedule 1 to the Act;**
- 6. The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised or unlawful processing, accidental loss, destruction and/or damage.**

Dated.....

Signed.....

Kate Lewis (Managing Director)
For Jubilee Managing Agency Ltd

Signed.....

Mick Gorrill (Assistant Commissioner, Regulatory Action Division)
For the Information Commissioner