

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Secretary of State for the Home Department
Home Office
2 Marsham Street
London
SW1P 4DF

I, David Normington, Permanent Secretary for the Home Department, of the Home Office, 2 Marsham Street, London SW1P 4DF, for and on behalf of the Secretary of State for the Home Department hereby acknowledge the details set out below and undertake to comply with the terms of the following undertaking:

1. The Secretary of State for the Home Department, 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 the Secretary of State for the Home Department 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 Commissioner was informed of the loss of an unencrypted memory stick holding, in all likelihood, the sensitive personal data of prisoners and offenders. The memory stick went missing whilst under the control of PA Consulting Group who was working under contract to the data controller and processing the data on its behalf. In response, an investigation into the circumstances was launched by the data controller's Departmental Security Unit resulting in a report dated 29 August 2008. In addition, Dr Stephen Hickey provided external scrutiny of the data controller's response to the data loss resulting in a report dated September 2008. Dr Hickey's terms of reference for the scrutiny was, amongst other things, to ensure appropriate action by the data controller has been taken or planned, and that lessons learned from the incident are comprehensive.
3. The Commissioner has considered both of the reports referred to in paragraph 2 above and considered the data controller's compliance with the provisions of the Act in light of these matters. The relevant provision of the Act is the Seventh Data Protection Principle. This Principle is set out in Schedule 1 Part 1 of the Act.
4. Following consideration of the remedial action that has been taken by the data controller and the fact that the data controller recognises the

seriousness of the matter, 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 Schedule 1 Part 1 of the Act and, in particular, that –

- **Where processing of personal data is carried out by a data processor on behalf of the data controller, the data controller shall take reasonable steps to ensure compliance with the guarantees made by the data processor in respect of the technical and organisational security measures governing the processing to be carried out.**
- **In taking reasonable steps the data controller shall carry out and document regular inspections of the security of the data processor's facilities for the processing of personal data and carry out regular audits of the data processor's processing activities to ensure compliance with the guarantees made by the data processor.**

Dated.....

Signed.....
For and on behalf of the Secretary of State for the Home Department

Signed.....
David Smith
Deputy Commissioner
For and on behalf of the Information Commissioner