

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Toshiba Information Systems (UK) Ltd

Toshiba Court
Weybridge Business Park
Addlestone Road
Weybridge
Surrey
KT15 2UL

I, Andy Bass, Chief Executive Officer, of Toshiba Information Systems (UK) Ltd, for and on behalf of Toshiba Information Systems (UK) Ltd hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Toshiba Information Systems (UK) 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 out by Toshiba Information Systems (UK) Ltd 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 informed by a concerned member of the public that individuals registered for an online competition hosted by the data controller could have their personal data accessed. A security fault with the incremental numbering of competition entrants registration URL, created the potential for access to other customer's personal data for a two month period. A total of 20 data subject's information was compromised as a result, including names, addresses, telephone numbers, email addresses and dates of birth.
3. It is the Commissioner's view that the organisational and technical security measures implemented by the data controller at the time of this security breach were not sufficient to detect a web design error made by their data processor that resulted in the online compromise of customer

personal data. The data controller had a written agreement in place with their data processor at the time of the incident.

4. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provision of the Act is the Seventh Data Protection Principle. This Principle is set out in Schedule 1 Part I 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 I of Schedule 1 to the Act, and in particular that:

1. The data controller will obtain sufficient guarantees from the data processor that it will conduct appropriate web application security tests in relation to any web applications which the data controller may instruct the data processor to create and which involve the processing of personal data ("Relevant Web Applications"), with the aim of preventing the compromise of customer personal data online;
2. The data controller shall take reasonable steps to ensure the data processor complies with all such guarantees in processing data for the purposes of Relevant Web Applications;
3. The data controller shall (i) consider data security in instructing the data processor to construct Relevant Web Applications, and (ii) take reasonable steps to ensure the data processor considers data security in constructing Relevant Web Applications;
4. The data controller shall implement appropriate and proportionate data security testing on each Relevant Web Application prior to launch;
5. The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing,

accidental loss, destruction, and/or damage.

Dated.....

Signed.....

Andy Bass
Chief Executive Officer
Toshiba Information Systems (UK) Ltd

Signed.....

Stephen Eckersley
Head of Enforcement
For and on behalf of the Information Commissioner