

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller:

Racing Post 5 Fleet Place London EC4M 7RD

I, Mr Alan Byrne, Chief Executive of the Racing Post, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

- The Racing Post 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 Racing Post 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.
- The Information Commissioner (the 'Commissioner') was informed of an incident taking place in October 2013, whereby the Racing Post website was subject to an internet-based SQL injection attack which gave the attacker access to a customer database.
- 3. Whilst there was no financial information stored in the database, the personal data accessed affected 677,335 data subjects. The data included customer registration details such as, name, address, password, date of birth and telephone number.
- 4. Following an investigation into the incident it was determined that the SQL injection attack was possible due to technical vulnerabilities in the website code. In addition, the data controller had failed to properly secure some of its systems by ensuring that up-to-date security patches were in place. It had also failed to arrange regular security testing.
- 5. During the Commissioner's investigation it was determined that the data controller had consulted security experts and procured penetration testing in 2007. However since that time there had been no steps taken to keep abreast of security developments. In the Commissioner's opinion, this placed the data at an unacceptable level of risk of inappropriate processing.

ICO Ref: ENF0522421



- 6. The Commissioner's investigation also determined that the storage of customer passwords as un-salted MD5 hash values was not appropriate. Overall the Commissioner determined that the data controller had not displayed an understanding of good security practice, nor the real risk presented by an internet-based attack.
- The Commissioner has considered the data controller's compliance with the provisions of the Act in 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.
- 8. 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 shall implement appropriate periodic security testing; the scope of this testing should be determined on the risk presented to the personal data the organisation processes, by no later than the 28 February 2015;
- (2) The data controller shall determine and implement, in accordance with industry standard, an appropriate and secure method of password storage, by no later than the 28 February 2015;
- (3) The data controller shall define and implement an appropriate software updates policy. This policy shall, by default, require software to be supported by security updates, and to have those security updates applied as soon as reasonably practicable but no later than 28 February 2015;
- Compliance with the data controller's policies on data protection and I.T security shall be appropriately and regularly monitored, by no later than the 28 February 2015;
- (5) The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and



unlawful processing, accidental loss, destruction, and/or damage, by no later than the 28 February 2015.

Signed Alan Byrne, Chief Executive Racing Post

Dated

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

Dated