mps marketing services limited

Dated: 10th May 2013

DATA SECURITY AGREEMENT

THIS AGREEMENT is made the day “data is uploaded to MPS”

BETWEEN:

1) **The Data uploader.** (the “Data Controller”)

2) **MPS Marketing Services Ltd,** Cattlemarket, Winford, Bristol, BS40 8HB, a company registered number 6360656 (the “Data Processor”)

WHEREAS

a) The Data Controller and the Data Processor have entered into a business relationship that is or will be the subject of a number of other agreements.

b) Paragraphs 11 and 12 of Part II of Schedule 1 of the Data Protection Act 1998 (“the Act”) place certain obligations upon a Data Controller to ensure that any Data Processor it engages provides sufficient guarantees to ensure that the processing of the data carried out on its behalf is secure.

c) This Agreement exists to ensure that there are sufficient security guarantees in place and that the processing complies with obligations equivalent to those of the 7th Data Protection Principle under the Act.

d) This Agreement is supplemental to any other separate agreement entered into between the parties and shall apply to any such agreement whether already in place or contemplated in the future (“the Other Agreements”) and introduces further contractual provisions to ensure the protection and security of data passed from the Data Controller to the Data Processor for processing.

In consideration of the obligations entered into by the parties in the course of their business relationship, **IT IS AGREED** as follows:

1. DEFINITIONS

In this agreement unless otherwise specified the following definitions will apply:

“Data” means personal data, including sensitive personal data, as defined in the Data Protection Act 1998 that is supplied by the Data Controller to the Data Processor.

“Project” means the business relationship existing between the Data Processor and the Data Controller that is the subject of the Other Agreements.

“Approved Employees” means those employees or subcontractors of the Data Processor who are involved in the Project.

2. SECURITY AND CONFIDENTIALITY OF THE DATA

2.1 The Data Processor will not make any use of the Data or allow any use of the Data except for the purpose of the Project and in particular (but not without limitation) will not use any of the Data for any other commercial purposes;

2.2 The Data Processor will hold the Data in the strictest confidence and will not disclose or allow the disclosure of any part of the Data, save as permitted in sub-clause 2.3 below to any third party without the Data Controller’s prior written consent which may be withheld or given on such terms and conditions as the Data Controller may consider appropriate;

2.3 The Data Processor will restrict access to the Data to such Approved Employees as strictly need to have access for the purpose of the Project and the Data Processor will impose upon all such persons obligations of confidentiality equivalent to those contained in this Agreement and the Data Processor will be responsible for ensuring that all such persons comply with these obligations;

2.4 The Data Processor shall use reasonable endeavours to safeguard the Data from unauthorised or unlawful processing or accidental loss, destruction or damage and acknowledges that it has implemented the technical and organisational measures specified in Schedule A, to prevent unauthorised or unlawful processing or accidental loss or destruction of the Data;

2.5 The Data Processor shall not use, reproduce or store any of the Data on an externally accessible computer or electronic information retrieval system, nor transmit it in any form or by any means whatsoever outside its usual place of business, unless specifically authorised to do so by the Data Controller.

2.6 The Data Processor shall take reasonable steps to ensure the reliability of all Approved Employees.

2.7 The Data Processor shall act only on written instructions from the Data Controller in relation to the Project and the Data, and, where reasonably necessary to do so, the Data Processor will forthwith confirm its understanding of the instruction with the Data Controller prior to execution, such execution not to be unreasonably delayed

2.8 The Data Processor shall ensure by written contract that any agent or subcontractor engaged by the Data Processor to process Data to which this Agreement relates also:

(a) Provides the Data Processor with a plan of the technical and organisational means it has adopted to prevent unauthorised or unlawful processing of or accidental loss of or destruction of the Data and;

(b) Confirms to the Data Processor the implementation of those means and;

(c) Enters into a contract with the Data Processor containing data security obligations which are no less onerous than those set out in this agreement.

3 TERMINATION

3.1 The undertakings contained in Clause 2 shall continue in force and effect and shall endure for the benefit of the Data Controller notwithstanding the completion of the Project (whether in whole or in part) until all Data and any copies thereof have been securely destroyed and removed from the Data Processor's computer systems. This destruction and removal of data will occur no earlier than 90 days after the completion of the Project, and no later than 180 days after the completion of the Project.

4 INDEMNITY

4.1 The Data Processor will be responsible for any breach of any of the terms of this Agreement by the Data Processor or any of its employees and the Data Processor shall be liable to indemnify and hold the Data Controller harmless against any losses, cost, claims, damages or expenses incurred by the Data Controller either as a result of the unauthorised disclosure by the Data Processor of any of the Data or as a result of the breach by the Data Processor of any of the terms of this Agreement but (other than for death or personal injury caused by the negligence of the Data Processor, its employees or agents) subject to a maximum value of £1,000,000.

5 WARRANTY

5.1 The Data Controller warrants that it has complied with the provisions of the Data Protection Act 1998 in relation to the Data and that all instructions given by the Data Controller to the Data Processor will be in compliance with the Data Protection Act 1998.

6 VARIATION

6.1 No purported variation of this Agreement shall be effective unless it is in writing and signed by or on behalf of each of the parties.

7 WAIVER

7.1 The failure of either party to enforce or exercise, at any time or for any period of time, any term or any right arising pursuant to this Agreement does not constitute, and shall not be construed as, a waiver of such term or right and shall in no way affect a party's right to enforce and exercise it.

8 INVALIDITY

8.1 To the extent that any provision of this Agreement is found by any court or competent authority to be invalid, unlawful or unenforceable in any jurisdiction, that provision shall be deemed not to be part of this Agreement nor shall it affect the enforceability of that provision in any other jurisdiction.

9 GOVERNING LAW AND JURISDICTION

9.1 This Agreement shall be governed by and construed in accordance with English law and the parties shall submit to the exclusive jurisdiction of the English Courts.

9.2 This Agreement shall become effective on the date first set forth above.

10 THIRD PARTIES

10.1 It is not intended that a third party shall have the right to enforce a provision pursuant to the Contracts (Rights of Third Parties) Act 1999.

SIGNED by duly authorised representative for and on behalf of

MPS Marketing Services Ltd

Jon Pinches

Jon Pinches - Director

SCHEDULE A

i Verify employees status prior to commencement of employment

ii Employees required to enter into confidentiality undertakings as part of their employment terms

iii Undertake an employee data security training programme

iv Password controlled access to systems

v Encryption and verification of parties communicating data

vi Controlled access to buildings and rooms

vii Adequate precautions against burglary, fire or natural disaster

viii Secure destruction of documents containing personal data

ix Back-up copies of the data stores securely and separately from the live files

x Procedures for full deletion before re-use of magnetic media (to prevent possible recovery by an unauthorised party)

xi Responsibility for the organisation’s security policy clearly placed on a particular person or department

xii Have an Information Security Policy.