

DATA TRANSFER AGREEMENT

11 AUGUST 2014

PAYMASTER (1836) LIMITED

AND

EQUINITI INDIA PRIVATE LIMITED

CONTENTS

1.	Definitions	1
2.	Details of the transfer.....	2
3.	Third-party beneficiary clause.....	2
4.	Obligations of the data exporter.....	3
5.	Obligations of the data importer.....	4
6.	Liability	5
7.	Mediation and jurisdiction	6
8.	Cooperation with the Information Commissioner.....	6
9.	Governing Law.....	7
10.	Variation of the contract.....	7
11.	Sub-processing.....	7
12.	Obligation after the termination of personal data processing services	Error! Bookmark not defined.

APPENDIX

ANNEX A - DETAILS OF THE TRANSFER.	9
ANNEX B - TECHNICAL AND ORGANISATIONAL SECURITY MEASURES.....	11

THIS AGREEMENT is made on 11 August 2014

BETWEEN

- (1) **PAYMASTER (1836) LIMITED** an English company (company number 3249700) whose registered office is at Sutherland House, Russell Way, Crawley, West Sussex RH10 1UH ("data exporter") and
- (2) **EQUINITI INDIA PRIVATE LTD** (PAN: AABC13514M) whose operating office is Block 10, 8th Floor, DLF IT Park, 1/124, Mt Poonamalle High Road, Ramapuram, Chennai, Tamil Nadu 600 089, India and

The parties to this Agreement have agreed that any processing of personal data undertaken for and on behalf of the data exporter within the Republic of India will be governed by the terms of this Agreement in order to ensure that adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals whose personal data is to be transferred by the data exporter for processing by the data importer in the Republic of India as specified in Annex A to this Agreement.

1. DEFINITIONS

- 1.1 In this Data Transfer Agreement, the following definitions will apply:
- (a) **Data Protection Act** means the Data Protection Act 1998;
 - (b) **Data Protection Directive** means Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
 - (c) **personal data, special categories of data, process/processing, controller, processor, data subject and Information Commissioner** shall have the same meaning as in the Data Protection Directive;
 - (d) **the data exporter** means the controller who transfers the personal data;
 - (e) **the data importer** means the processor who agrees to receive from the data exporter personal data intended for processing on its behalf after the transfer in accordance with its instructions and the terms of this Data Transfer Agreement and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
 - (f) **the Information Commissioner** means the Commissioner as appointed from time to time under the Data Protection Act, such Commissioner being the Information Commissioner in England for the purposes of the Data Protection Directive;
 - (g) **the sub-processor** means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer

personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with its instructions, the terms of this Data Transfer Agreement and the terms of the written subcontract;

- (h) **the applicable data protection law** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (i) **technical and organisational security measures** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

- 1.2 References to Acts and other legislation are to such legislation as amended, extended or re-enacted (whether before or after the date of this Agreement) and any subordinate legislation made under that legislation.

2. **DETAILS OF THE TRANSFER**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Annex A which forms an integral part of this Data Transfer Agreement.

3. **THIRD-PARTY BENEFICIARY CLAUSE**

- 3.1 The data subject can enforce against the data exporter this clause 3, clause 4(b) to clause 4(i), clause 5(a) to clause 5(e) and clause 5(g) to clause 5(j), clause 6.1 and clause 6.2, clause 7, clause 8.2 and clause 9 to clause 12 as third-party beneficiary.
- 3.2 The data subject can enforce against the data importer this clause 3.2, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2 and clause 9 to clause 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
- 3.3 The data subject can enforce against the sub-processor this clause 3.3, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2, and clause 9 to clause 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and

obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under this Data Transfer Agreement.

- 3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. OBLIGATIONS OF THE DATA EXPORTER

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and this Data Transfer Agreement;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Annex B to this Data Transfer Agreement;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any sub-processor pursuant to clause 5(b) and clause 8.3 to the data protection Information Commissioner if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of this Data Transfer Agreement, with the exception of Annex B and a summary

description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with this Data Transfer Agreement, unless this Data Transfer Agreement or the contract contain commercial information, in which case it may remove such commercial information;

- (i) that, in the event of sub-processing, the processing activity is carried out in accordance with clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subjects as the data importer under this Data Transfer Agreement; and
- (j) that it will ensure compliance with clause 4(a) to clause 4(i).

5. OBLIGATIONS OF THE DATA IMPORTER

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and this Data Transfer Agreement; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by this Data Transfer Agreement, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Annex B before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
 - (ii) any accidental or unauthorised access; and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to

abide by the advice of the Information Commissioner with regard to the processing of the data transferred;

- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by this Data Transfer Agreement which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Information Commissioner;
- (g) to make available to the data subject upon request a copy of this Data Transfer Agreement, or any existing contract for sub-processing, unless this Data Transfer Agreement or contract contain commercial information, in which case it may remove such commercial information, with the exception of Annex B which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub-processor will be carried out in accordance with clause 11; and
- (j) to send promptly a copy of any sub-processor agreement it concludes under this Data Transfer Agreement to the data exporter.

6. LIABILITY

- 6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in clause 3 or in clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
- 6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or its sub-processor of any of their obligations referred to in clause 3 or in clause 11 because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in clause 3 or in clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under this Data Transfer Agreement as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under this Data Transfer Agreement.

7. MEDIATION AND JURISDICTION

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under this Data Transfer Agreement, the data importer will accept the decision of the data subject:

- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the Information Commissioner;
- (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. COOPERATION WITH THE INFORMATION COMMISSIONER

8.1 The data exporter agrees to deposit a copy of this contract with the Information Commissioner if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the Information Commissioner has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in clause 5(b).

9. GOVERNING LAW

This Data Transfer Agreement shall be governed by the law of the Member State in which the data exporter is established, namely English Law.

10. VARIATION OF THE CONTRACT

The parties undertake not to vary or modify this Data Transfer Agreement. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict this Data Transfer Agreement.

11. SUB-PROCESSING

- 11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under this Data Transfer Agreement without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under this Data Transfer Agreement, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under this Data Transfer Agreement. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
- 11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under this Data Transfer Agreement.
- 11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely English law.
- 11.4 The data exporter shall keep a list of sub-processing agreements concluded under this Data Transfer Agreement and notified by the data importer pursuant to clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection Information Commissioner.

12. OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA PROCESSING SERVICES

12.1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the Information Commissioner, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

This agreement has been entered into on the date stated at the beginning of it.

DATA EXPORTER

Signed by MARTYN HINDLEY for and on behalf of
Paymaster (1836) Limited

Signature: 
DIRECTOR

Date: 12/08/2014

DATA IMPORTER

Signed by DAVID DUNBAR MAWHINNEY for and on
behalf of Equiniti India Private Limited

Signature: 
DIRECTOR

Date: 29/7/2014

Annex A.

This Annex forms part of this Data Transfer Agreement and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Annex A.

The data exporter is;

Paymaster (1836) Limited whose registered office is at Sutherland House, Russell Way, Crawley, West Sussex RH10 1UH ("Paymaster").

Paymaster is a provider of pensions software, outsourced pension administration, insurance and payment services to clients and customers. Equiniti Group for the purposes of this Agreement includes Paymaster and any subsidiary or holding company of Paymaster and each and any subsidiary of a holding company of Paymaster.

The data importer is:

Equiniti India Private Limited ("Equiniti India") whose operating office is Block 10, 8th Floor, DLF IT Park, 1/124, Mt Poonamalle High Road, Ramapuram, Chennai, Tamil Nadu 600 089, India.

Equiniti India is a provider of application development, application management and infrastructure management services across the Equiniti Group.

The Data subjects are:

The personal data transferred concern the following categories of data subjects:

- Customers and clients of Equiniti Group
- Equiniti Group customers' and clients' current or former employees, shareholders, beneficial shareholders, customers, contractors or agents ("Customer Group")
- Staff including volunteers, agents, temporary and casual workers of Equiniti Group (previous and prospective employers of the staff and references)
- Suppliers of Equiniti Group
- Relatives, guardians and associates of the data subject
- Advisers, consultants and other professional experts of Equiniti Group or Customer Group
- Complainants, correspondents and enquiries of Equiniti Group or Customer Group
- Members or supporters of Equiniti Group
- Named individuals or corporate bodies supplied for the purpose of verification

Categories of data

The personal data transferred concern the following categories of data:

- Personal Details
- Financial Details
- Goods or Services provided

Special Categories

The personal data transferred concern the following special categories of data (please specify)

- NONE

Processing operations

The personal data transferred will be subject to the following basic processing activities:

Remote access is available to Equiniti India to enable the provision of application development, application management and infrastructure services for the data exporter's pensions software, outsourced pension administration, insurance and payment services. The IT support teams do not undertake the processing of any business transactions. They may collate statistics on system and user activities for Management Information reports.

Annex B.

This Annex B forms part of this Data Transfer Agreement and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with clause 4 (d) and clause 5 (c) (or documents/legislation attached):

Information Security at Equiniti India Private Limited ("Equiniti India") has a set of controls including policies, practices, procedures and organizational structures to protect the confidentiality, integrity and availability of its own and its clients' information. Furthermore, Equiniti India has a security assessment program where periodic independent audits are undertaken ensuring continuing effectiveness:

- at a minimum of once per year Equiniti India employees are background checked to the Equiniti Group's required standard, and at a minimum of once per year required to sign Terms of Employment as per defined policies and processes. Terms of Employment contains clauses addressing compliance to Equiniti India policies on Confidentiality, Information Property, Data Privacy
- Equiniti India employees undergo a periodic security awareness training, at a minimum of once per year, focused on essential security policies and emphasising on the user responsibilities related to incident management, data privacy, business continuity and information security
- A disciplinary process is documented and communicated to employees when they join Equiniti India Private Limited.

Business Continuity Planning

- Equiniti India Private Limited has an established Business Continuity Management (BCM) strategy where the objective is to mitigate the disruption caused by disasters and security failures to an acceptable level through a combination of preventive and recovery controls. Business Risk Impact Assessment for all primary and secondary business functions are documented and reviewed annually, and validated quarterly. The BCM covers the organization's facilities, equipment, personnel and processes including information processing depending on the business continuity needs.
- In line with the Equiniti Group's standard approach, Equiniti India has adopted a formal strategy to Business Continuity and Disaster Recovery (BCDR) of its delivery centre which mitigate identified risks to the facility through the ability to revert all services to the Equiniti facilities within the UK without any undue delay.

Physical & Environmental Security

- Equiniti India facilities have four levels/zones of security as follows :
 - o Level 0 - access to building premises (controlled by security guards vetting business passes)
 - o Level 1 - access to Reception Lobby (controlled by security guards with access control readers)
 - o Level 2 - access to all Open work areas (controlled by turn styles with access control readers)
 - o Level 3 - access to Hub Rooms and Protected Bays (limited access controlled through access control readers)
- CCTV are utilized at entry / exit points and prominent locations and monitored 24x7
- Employees display their office identity cards while they are in office
- Facilities have clearly defined and marked fire evacuation routes, fire exit points and assembly areas
- Facilities have required Infrastructure support for ACs and power backup, using UPS with power protection to the Equiniti India office level, and diesel generators to the office complex.

Technical Measures

Workstation Security

- Standard Equiniti Workstation images
- Microsoft Forefront anti-virus and firewalls
- Unique user IDs, Password controls with time expiry implemented
- USB, FDD and CDROM disabled
- Centralised Patch Management using Equiniti Group approved tools and practices
- Restricted Internet access using Equiniti proxy servers
- Equiniti Policies enforced using Active Directory Group Policies
- Central monitoring and control of Antivirus
- Workstations support local telephony and a locked-down Terminal Services session into the UK-based environments where all activities take place.

Server Security

- Equiniti Security Policy & Standards implemented
- System Security Policy deployed
- Equiniti Standard Server Image
- Forefront Antivirus Software for Servers
- System Security Policies enforced using Windows Domains/ Active Directory
- Access Control enforced - Least Privilege Principle implemented
- Periodic Log reviews performed
- Centralised Patch Management Process
- Servers are present just to support the local telephony and PC infrastructure (patching/AD etc), and the routing of Terminal Services session into the UK-based environments where all activities take place

Network Security

- Secure Network design Architecture built to Equiniti Group standards
- Network equipment hardened using Equiniti Security Baseline Standards
- VPN Solution (Encryption) implemented for WAN Connectivity
- Multiple layer of Network Security
 - o Access Control List on Perimeter Router
 - o External Firewall (Internet Facing) in Fallover mode.
 - o Internal Firewall in Fallover mode – (Different product vendors for External and Internal Firewalls)
 - o Diverse routing of external connectivity to Equiniti in UK