ANNEXURE
DATA PROCESSING TERMS

This Data Processing Terms ("DPA") is to govern the processing of the Personal Data between the Parties to the Agreement each on behalf of themselves and their Affiliates (together, the "Parties") and shall form an integral part of the Agreement.

1. ORDER OF PRECEDENCE

All capitalized terms not otherwise defined in this DPA shall have the meaning assigned to them in the Agreement. In the event of any conflict or inconsistency, this DPA shall supersede and prevail over any conflicting terms in the Agreement.

2. DEFINITIONS

"Affiliate" means in relation to a party, a corporation owned or controlled by the party or which owns or Controls the party or which is owned or controlled by a parent corporation which also owns that party;

"Agreement" means commercial agreement entered between the Parties including the schedules, annexes, appendices and any amendments and variations made thereto;

"Applicable Law" means with respect to any person or thing, supranational, national, state, provincial, municipal or local law, common law, regulation, directive, guideline, constitution, act of parliament, ordinance, treaty, convention, by-law, circular, guidance, notice, codes, rule (including the rules of any applicable stock exchange), order, injunction, judgment, decree, arbitral award, ruling, finding or other similar requirement enacted, adopted, promulgated or applied by an Authority, including any amendments, re-enactment or replacement of it, that has the force of law with respect to such person or thing in any jurisdiction;

"Authority" includes any supranational, national, state, municipal or local government, governmental, semi-governmental, intergovernmental, regulatory, judicial or quasi-judicial body, agency, department, entity or authority, stock exchange or self-regulatory organisation established under statute and shall include persons exercising executive, legislative, judicial, regulatory or administrative functions of or pertaining to government;

"Company" means a corporate entity which has an Agreement entered with TIME and the scope of which inter alia involves processing of Personal Data solely on behalf of TIME and for the purpose of the Agreement. To the extent that the Company processes TIME Data, the Company is deemed a Data Processor (as defined in the PDPA);

"Control" means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person or entity or other control over a person or entity, whether through the ownership of voting securities, by contract or otherwise;

"Data Processing Operations" means collecting, recording, holding or storing Personal Data or carrying out any operation or set of operations on Personal Data, including:

(a) the organization, adaptation, modification or alteration of Personal Data;
(b) the retrieval, consultation or use of Personal Data;
(c) the disclosure of Personal Data by transmission, transfer, dissemination or otherwise making available; or
(d) the alignment, combination, correction, erasure or destruction of Personal Data;

"Data Subject" means an individual who is the subject of the Personal Data;

"PDPA" means the Malaysian Personal Data Protection Act 2010 and all relevant regulations, standards, code of practice and guidelines issued by the Malaysian Data Protection Authority;

"Personal Data" means any information that relates directly or indirectly to a Data Subject, who is identified or identifiable from that information or from that and other information, including any sensitive personal data and expression of opinion about the Data Subject.

"Services" means the products and/or services provided by the Company to TIME pursuant to the Agreement.

"TIME" means TIME Dotcom Berhad and its subsidiaries, associates and Affiliates;

"TIME Data" means Personal Data including but is not limited to, the data, text, drawings, diagrams, plans, statistics or images (together with any database made up of any of these) which are embodied in any electronic, magnetic, electromagnetic, optical, tangible or other media that is directly or indirectly supplied by TIME to the Company under the Agreement or which the Company is required to process pursuant to the Agreement.

3. DETAILS OF THE PROCESSING

3.1. *Nature and purpose.* The Company will only process the Personal Data as necessary to perform its obligations under the Agreement and as further instructed by TIME in writing.

3.2. *Duration.* Notwithstanding the Term of the Agreement, this DPA shall be effective from the earlier the effective date of the Agreement or such time the Company processes or has access to the Personal Data, and shall remain in force for as long as the Company processes or has access to the Personal Data
or as otherwise agreed-upon in writing.

3.3. *Categories of Data Subjects.* TIME may provide the Company with TIME Data which may include without limitation, Personal Data relating to the following categories of Data Subjects: consumers or users of goods and/or Services provided, administered, or operated by TIME or any of its Affiliate; TIME personnel; and/or third parties that have, or may have, a commercial relationship with TIME (e.g., advertisers, customers, prospects, business partners, and/or content providers etc).

3.4. *Types of Personal Data.* TIME may provide the Company with Personal Data generated, shared, uploaded, collected from, or provided by consumers or users of goods and Services provided, administered, or operated by TIME or any of its Affiliate; Personal Data of TIME personnel generated in the normal course of staff administration, e.g., routine employee data; and/or the Personal Data relating to external third parties with whom TIME has, or may develop, a commercial relationship (e.g., advertisers, customers, prospects, business partners, and/or content providers etc).

4. COMPLIANCE

4.2. *Obligations.* With respect to any TIME Data that is processed by the Company for the purpose of fulfilling Company's obligations to TIME under the Agreement, the Company shall:

4.2.1. at all times comply with the PDPA and all applicable Data Protection legislation In other jurisdiction (collectively "Personal Data Legislation") in respect of the Data Processing Operations;

4.2.2. Subject to the clause below, only process (e.g., receive, retain, use, sell, transfer, disclose, etc.) TIME Data pursuant to the specific purpose(s) described in and/or contemplated by the Agreement, and only in accordance

with instructions contained in that Agreement, or as otherwise received from TIME in writing;

4.2.3. not do or omit to do anything that would cause TIME to contravene, or that would result in TIME contravening, any Personal Data Legislation; and

4.2.4 Where the Company is obliged by Applicable Law to process any TIME Data that is Personal Data other than in accordance with Clause 3 above, the Company must inform TIME of that obligation, providing:
(i) as much advance notice of any such processing as is reasonably possible;
(ii) a description of the nature and timing of any such processing; and
(iii) details of the applicable law that requires such processing.

4.2. *Insurance.* The Company shall take out and maintain insurance to protect against the risks of data breach including any cyber incident in which TIME Data has or may have been compromised and comply with the provisions of that insurance.

4.3. *Indemnity.* The Company shall fully indemnify and hold TIME harmless from all claims, liabilities, costs, expenses and damages and loss resulting from the Company's failure to comply with the requirements set out in this DPA and laws applicable to the Company's data processing activities.

4.4. *Material Breach.* Any non-conformity with the requirements set out in this DPA shall be regarded as a material breach of the Agreement by the Company.

5. ACCESS REQUESTS

5.1. *Data Subject.* Insofar as is possible, the Company shall provide, at no additional cost to TIME, any resources and assistance reasonably requested by TIME in order to allow TIME to comply with its obligations under PDPA including to Data Subjects (or equivalent) who exercise their rights under PDPA.

5.2. *Assistance.* Taking into account the nature of the processing and the information available to the Company, the Company shall provide, at no additional cost to TIME, any resources and assistance reasonably requested by TIME in order to allow TIME to comply with its obligations under PDPA and its internal policies and procedures including assisting TIME with the performance of any relevant data protection impact assessments.

5.3. *Audits.* Without prejudice to TIME's rights in the Agreement, the Company shall provide such assistance and information as TIME reasonably requires in order to demonstrate the Company's compliance with its obligations and permit TIME or its external advisers and representatives (subject to reasonable notice) (or any relevant Authority and regulatory body) to inspect and audit the data processing activities carried out by the Company, including access to the premises, records, and personnel of the Company (or the Company's contractors and/or Sub-Processors).

5.4. *Infringement.* The Company shall inform TIME immediately, if, in the Company's reasonable opinion, any instruction from TIME infringes any applicable Data Protection Legislation.

5.5. *Records.* The Company shall maintain records as required under PDPA of all processing activities carried out pursuant to the Agreement and make such records available to TIME or its representatives on reasonable demand and notice.

5.6. *Notification.* The Company shall notify TIME immediately if the Company receives any investigation, communication, inspection, audit, administrative sanction, or fine, from any Authority, or any claim, proceedings or complaint by a Data Subject directly (If any), which relates directly or indirectly to the processing of TIME Data under the Agreement.

6. INCIDENT MANAGEMENT AND NOTIFICATION

6.1. *Notice.* In relation to any breach involving TIME Data, the Company shall notify TIME in writing without undue delay (and in any event within six (6) hours) of the discovery by the Company of any actual or suspected data breach involving TIME Data, whether or not such a breach is the responsibility of the Company. The notification to TIME must include at least inter alia: (a) a description of the nature of the breach, including where possible the categories, approximate number of data subjects concerned and the identity of each data subject affected; (b) the name and contact details of the Company contact from whom more information can be obtained; (c) a description of the measures taken or proposed to be taken to address the breach, including, where appropriate, measures to mitigate its possible adverse effects; and (d) any other information TIME reasonably requests relating to the breach, to allow TIME to meet any reporting obligations or inform Data Subjects of the breach under the PDPA.

6.2. *Assistance.* the Company shall provide TIME with all resources and assistance as are required by TIME for it to investigate a breach and enable TIME to notify the relevant Authority and regulatory body (or bodies) and/or the relevant Data Subjects of such a breach, as applicable.

6.3. Business Continuity and Disaster Recovery. The Company shall develop and maintain the following:-

(a) business continuity plans ("BCP(s)") based on business continuity requirements consistent with the recognized standard or equivalent to meet obligations under the Agreement in the event of a business interruption or disaster caused by the material loss of operational resources due to a natural or man-made event; and

(b) the recovery of critical technology systems and periodically perform testing in the primary or designated recovery environment for such critical technology systems.

The Company shall make reasonable attempts under the circumstances to contact TIME in a timely manner in the event of a business interruption that materially affects TIME, if any, and to communicate plans for recovery from a business interruption and resumption of normal business operations as soon as practicable.

7. SECURITY

7.1. *Controls.* Company shall ensure and maintain appropriate, adequate, and reasonable security procedures and practices, and take technical and organizational measures to protect TIME Data from a confirmed or reasonably suspected accidental or unlawful use, access, destruction, damage, alteration, or disclosure of TIME Data. Such procedures and practices shall be equivalent to the industry standard for information security management and shall not materially decrease throughout the Company's access to and processing of TIME Data.

7.2. Access Requests. At TIME's request, Company will promptly provide an up-to-date written physical, security procedures and practices, and technical and organizational security measures employed by the Company for processing TIME Data. These measures shall be appropriate to the level of risk presented by the processing, appropriate to the nature of the TIME Data, and to the harm which might result from a personal data breach affecting the TIME Data.

7.3. *Security Protection.* Company agrees to maintain the following minimum technical and organisational measures:

A. Access Control to Processing Areas and Systems.

Company shall prevent unauthorized persons from gaining access to the data processing equipment, system or application where the TIME Data are processed or used. These include:

- Securing the data processing equipment;
- Establishing access authorizations for staff and third parties;
- Individual authentication credentials such as user ID and passwords;
- Where applicable. securing the data center where personal data are hosted by a security alarm system, and other appropriate security measures;
- Automatic time-out of user terminal if left idle, identification and password required to reopen;
- Staff policies in respect of each staff access rights to data, informing staff about their obligations and the consequences of any violations of such obligations, to ensure that staff will only access Personal Data and resources required to perform their job duties and training of staff on applicable privacy duties and liabilities;
- All access to data content is logged, monitored, and tracked; and
- Use of state-of-the-art encryption technologies.

B. Transmission Control.

Company shall prevent unauthorized persons from gaining access to the TIME Data. This includes:

- Use of state-of-the-art firewall and encryption technologies to protect the gateways and networks through which the data travels; and
- As far as possible, logging, monitoring, and tracking all data transmissions.
- take all necessary steps to prevent any malware being introduced into any software or onto any of the TIME systems or any information technology equipment (including computer hardware), systems or networks used by the Company to carry out Data Processing Operations for TIME or to supply the Services to TIME.

C. Accountability.

Company shall protect the data and monitor its system administrators. This includes:

- Adoption of suitable measures to register system administrators' access logs and keep them secure and accurate. destruction or loss. This includes:
  - Protecting data from accidental destruction or loss by backing up ;
  - Identifying any person that carries out a data recovery procedure;
  - Recording any detected security incident; and
  - Monitoring system administrators and to ensure that they act in accordance with instructions received.

8. CONFIDENTIALITY.

8.1. *Personnel.* Company shall ensure that only those authorised employees, agents, and consultants of the Company (and of any Company authorised Sub-Processor) that need to know, or need to have access, have access to the TIME Data and that they are under confidentiality obligations with respect to TIME Data. Such confidentiality obligations shall include, at a minimum, receiving appropriate training on their data protection responsibilities and executing written confidentiality agreements that survive the termination of the person's engagement.

8.2. *Statements.* Unless required by Applicable Law, the Company shall not make any statement (or provide any documents) about matters concerning the Agreement, or the processing of the TIME Data under the Agreement, without the written approval of TIME. Where the Company is required under Applicable Law to make any such statement (or provide any documents), the Company shall first provide to TIME a

copy of any such statements (or documents), unless prohibited by Applicable aw, and shall co-operate with, and take account of any comments of TIME prior to such legally required disclosure.

9. RETURN AND DELETION OF TIME DATA.

9.1. *Requests.* Upon written request from TIME, Company shall promptly (but in any event not later than thirty (30) calendar days) return all TIME Data transferred and any copies to TIME or delete any particular or all TIME Data in its possession, and certify in writing to TIME that it has complied with the requirements of this clause, provided that, if Company is required to maintain any TIME Data by law, or by the terms of a separate agreement with TIME, Company shall provide a written statement to TIME that identifies the TIME Data that was not deleted and the reason for the non-deletion. In that case, the Company shall hold such TIME Data in accordance with its obligations under this Agreement, and shall not process such TIME Data for any purpose other than as required by law.

9.2. *Expiration or Termination.* Without prejudice to TIME's rights in the Agreement, at the choice of TIME, Company shall delete, destroy, or return all TIME Data to TIME after the termination or expiration of the Agreement.

10. SUB-PROCESSORS

10.1. *Consent.* Company shall not subcontract or otherwise engage any sub-processor, subcontractors and other supply chain arrangements to carry out processing activities with respect to the TIME Data ("Sub-Processor") without the prior written consent of TIME, which shall not be unreasonably withheld and which may be conferred in the Agreement.

10.2. *Requirements.* Where use of a Sub-Processor has been approved by TIME, Company shall:

10.2.1. ensure that It has conducted appropriate due diligence on its Sub-processors (or third parties, as the case may be).

10.2.2 ensure that it enters into a written contract with the Sub-Processor which imposes on each party obligations at least equivalent to and no less protective than those imposed in this DPA.

10.2.2. ensure that each Sub-Processor complies with PDPA and applicable Data Protection Legislation within its jurisdiction.

10.2.3. unless otherwise specified in the Agreement, the Company remain fully liable to TIME for the acts and omissions of its Sub-Processors to the same extent the Company shall be liable under the terms of this DPA.

11. TRANSFERS

11.1 The Company shall not transfer or remotely access TIME Data without the prior written consent of TIME. The Company shall ensure that any transfer of, or remote access to TIME Data does not contravene any provisions of this DPA and the Agreement or any applicable laws and that such TIME Data is adequately protected at all times. All transfer of such TIME Data shall be encrypted or be secured in other ways.

12. NON-CORFORMITY

12.1 Any non-conformity with the requirements set out in this DPA Terms shall be regarded as a material breach of the Agreement by the Company.