timeTec

DATA PROCESSING ADDENDUM (DPA)
(GDPR and EU Standard Contractual Clauses)
(Version January 2023)

This Data Processing Addendum ("DPA"), forms part of the Agreement or Terms of Service between the Customer and TimeTec Cloud Sdn. Bhd. ("TimeTec") and shall be effective on the date Customer signed to accept or the parties otherwise agreed to this DPA ("Effective Date"). This Data Processing Addendum reflects the parties' agreement with respect to the terms governing the processing and security of Customer Data under the applicable Agreement.

1. Definitions

1.1. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. In this Data Processing Addendum, the following terms shall have the meanings set out below, unless stated otherwise:

a. "**Affiliate**" means any entity controlling, controlled by, or under common control with a party, where "control" is defined as: (a) the ownership of at least fifty percent (50%) of the equity or beneficial interests of the entity; (b) the right to vote for or appoint a majority of the board of directors or other governing body of the entity; or (c) the power to exercise a controlling influence over the management or policies of the entity.

b. "**Agreed Liability Cap**" means the maximum monetary or payment-based amount at which a party's liability is capped under the applicable Agreement, either per annual period or event giving rise to liability, as applicable.

c. "**Agreement**" means TimeTec's Terms of Service (or App Terms, whichever applicable) which govern the provision of the Services to Customer, as such terms may be updated by TimeTec from time to time.

d. "**Customer Data**" means data submitted, stored, sent or received via the Services by Customer, its Affiliates or End Users.

e. "**Customer Personal Data**" means personal data contained within the Customer Data.

f. "**Data Controller**" means an entity that determines the purposes and means of the processing of Personal Data.

g. "**Data Incident**" means a breach of TimeTec's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by TimeTec. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

h. "**Data Processo**r" means an entity that processes Personal Data on behalf of a Data Controller.

i. "**Data Protection Laws and Regulations**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

j. "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

k. “**EEA**” means the European Economic Area.
l. “**European Data Protection Legislation**” means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).
m. “**GDPR**” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
n. “**Standard Contractual Clauses**” or “**SCCs**” means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR.
o. “**Notification Email Address**” means the Account Owner Email Address (by default, email address used to sign up for the TimeTec account).
p. "**Personal Data**" means any information relating to an identified or identifiable natural person.
q. "**Processing**" has the meaning given to it in the GDPR and "process", "processes" and "processed" shall be interpreted accordingly.
r. “**Security Documentation**” means all documents and information made available by TimeTec under Section 5.5.1 (Reviews of Security Documentation).
s. “**Security Measures**” has the meaning given in Section 5.1.1 (TimeTec’s Security Measures).
t. “**Services**” means any product or service provided by TimeTec to Customer pursuant to the Agreement.
u. “**Subprocessors**” means third parties authorized under this Data Processing Addendum to have logical access to and process Customer Data in order to provide parts of the Services and related technical support.
v. “**Term**” means the period from the Effective Date until the end of TimeTec’s provision of the Services under the applicable Agreement, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which TimeTec may continue providing the Services for transitional purposes.

1.2. The terms “data importer” and “data exporter” have the meanings given in the **Standard Contractual Clauses**.

2. Duration of Data Processing Addendum

This Data Processing Addendum will take effect on the Effective Date and, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon, deletion of all Customer Data by TimeTec as described in the Agreement.

3. Processing of Personal Data

3.1 Roles of the Parties

The parties acknowledge and agree that with regard to the Processing of Customer Personal Data, Customer is the Controller, TimeTec is the Processor and that TimeTec will engage Subprocessors pursuant to the requirements set forth in Section 9 “Subprocessors” below.

3.2 Customer’s Processing of Personal Data

Customer shall, in its use of the Services, Process Customer Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer’s instructions for the Processing of Customer Personal Data shall comply with Data Protection Laws and Regulations.

Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data.

3.3 TimeTec's Processing of Personal Data

TimeTec shall treat Customer Personal Data as Confidential Information and shall only Process Customer Personal Data on behalf of and in accordance with Customer's documented instructions. Customer hereby instructs TimeTec to process Customer Personal Data for the following purposes: (i) Processing in accordance with the Agreement and in providing related technical support; (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

3.4 Details of the Processing

The parties acknowledge and agree that the subject matter and details of the processing are described in **Attachment 2**.

4. Return and Deletion of Customer Data

TimeTec shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in the Agreement.

You can exercise the applicable rights by submitting your request through https://www.timeteccloud.com/account-deletion.

If the Customer Data has been submitted to us by or on behalf of a TimeTec customer and you wish to exercise any rights you may have under applicable Data Protection Laws and Regulations, please inquire with the applicable customer directly, as described in **3.2 Customer's Processing of Personal Data**.

5. Data Security

5.1. TimeTec's Security Measures, Controls and Assistance

5.1.1. TimeTec's Security Measures

TimeTec will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in **Attachment 1, Appendix 2** (the "Security Measures") of the Addendum. As described in **Attachment 1, Appendix 2**, the Security Measures include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of TimeTec's systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. TimeTec may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

5.1.2. Security Compliance by TimeTec Staff

TimeTec will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Sub-processors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.1.3. TimeTec's Security Assistance

Customer agrees that TimeTec will (taking into account the nature of the processing of Customer Personal Data and the information available to TimeTec) assist Customer in ensuring compliance with any of Customer's obligations in respect of security of personal data and personal data breaches, including if applicable Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by:

(a) implementing and maintaining the Security Measures in accordance with Section 5.1.1 (TimeTec's Security Measures);
(b) complying with the terms of Section 5.2 (Data Incidents); and
(c) providing Customer with the Security Documentation in accordance with Section 5.5.1 (Reviews of Security Documentation) and the information contained in the applicable Agreement including this Data Processing Addendum.

5.2. Data Incidents (Personal Data Breach)

5.2.1. Incident Notification

If TimeTec becomes aware of a Data Incident, TimeTec will: (a) notify Customer of the Data Incident promptly and without undue delay; and (b) promptly take reasonable steps to minimize harm and secure Customer Data.

5.2.2. Details of Data Incident

Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps TimeTec recommends Customer take to address the Data Incident.

5.2.3. Delivery of Notification

Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address or, at TimeTec's discretion, by direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for ensuring that the Notification Email Address is current and valid.

5.2.4. No Assessment of Customer Data by TimeTec

TimeTec will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Data Incident(s).

5.2.5. No Acknowledgment of Fault by TimeTec

TimeTec's notification of or response to a Data Incident under this Section 5.2 (Data Incidents) will not be construed as an acknowledgement by TimeTec of any fault or liability with respect to the Data Incident.

5.3. Customer's Security Responsibilities and Assessment

5.3.1. Customer's Security Responsibilities

Customer agrees that, without prejudice to TimeTec's obligations under Section 5.1 (TimeTec's Security Measures, Controls and Assistance) and Section 5.2 (Data Incidents):
(a) Customer is solely responsible for its use of the Services, including:
(i) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Data;
(ii) securing the account authentication credentials, systems and devices Customer uses to access the Services; and

(iii) backing up its Customer Data; and

(b) TimeTec has no obligation to protect Customer Data that Customer elects to store or transfer outside of TimeTec's and its Subprocessors' systems (for example, offline or on-premise storage).

5.3.2. Customer's Security Assessment

(a) Customer is solely responsible for reviewing the Security Documentation and evaluating for itself whether the Services, the Security Measures and TimeTec's commitments under this Section 5 (Data Security) will meet Customer's needs, including with respect to any security obligations of Customer under Data Protection Laws and Regulations, as applicable.

(b) Customer acknowledges and agrees that the Security Measures implemented and maintained by TimeTec as set out in Section 5.1.1 (TimeTec's Security Measures) provide a level of security appropriate to the risk in respect of the Customer Data.

5.4. Security Certifications and Reports

TimeTec operates an information security management system (ISMS) for the Services in accordance with the ISO 27001 international standard and has achieved the certification from an independent third party.

5.5. Reviews and Audits of Compliance

5.5.1. Reviews of Security Documentation

Upon Customer's written request, and subject to the confidentiality obligations set forth in the Agreement, TimeTec shall make available to Customer that is not a competitor of TimeTec (or Customer's independent, third-party auditor that is not a competitor of TimeTec) a copy of TimeTec's most recent third-party audits or certifications, as applicable.

5.5.2. Customer's Audit Rights

(a) If the European Data Protection Legislation applies to the processing of Customer Personal Data, TimeTec will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify TimeTec's compliance with its obligations under this Data Processing Addendum in accordance with Section 5.5.3 (Additional Business Terms for Reviews and Audits). TimeTec will contribute to such audits as described in Section 5.4 (Security Certifications and Reports) and this Section 5.5 (Reviews and Audits of Compliance).

(b) If Customer has entered into Standard Contractual Clauses as described in Section 8.2 (Transfers of Data Out of the EEA), TimeTec will, without prejudice to any audit rights of a supervisory authority under such Standard Contractual Clauses, allow Customer or an independent auditor appointed by Customer to conduct audits as described in the Standard Contractual Clauses in accordance with Section 5.5.3 (Additional Business Terms for Reviews and Audits).

(c) Customer may also conduct an audit to verify TimeTec's compliance with its obligations under this Data Processing Addendum by reviewing the Security Documentation (which reflects the outcome of audits conducted by TimeTec's Third Party Auditor).

5.5.3. Additional Business Terms for Reviews and Audits

(a) Customer must send any requests for reviews under Section 5.5.1 or audits under Section 5.5.2(a) or 5.5.2(b) to TimeTec by postal mail to TimeTec's headquarter office address as indicated on our website's **Contact Us** section.

(b) Following receipt by TimeTec of a request under Section 5.5.3(a), TimeTec and Customer will discuss and agree in advance on: (i) the reasonable date(s) of review under Section 5.5.1; and (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under Section 5.5.2(a) or 5.5.2(b).

(c) TimeTec may charge a fee (based on TimeTec's reasonable costs) for any audit under Section 5.5.2(a) or 5.5.2(b). TimeTec will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

(d) TimeTec may object in writing to an auditor appointed by Customer to conduct any audit under Section 5.5.2(a) or 5.5.2(b) if the auditor is, in TimeTec's reasonable opinion, not suitably qualified or independent, a competitor of TimeTec, or otherwise manifestly unsuitable. Any such objection by TimeTec will require Customer to appoint another auditor or conduct the audit itself.

5.5.4. No Modification of Standard Contractual Clauses

Nothing in this Section 5.5 (Reviews and Audits of Compliance) varies or modifies any rights or obligations of Customer or TimeTec under any Standard Contractual Clauses entered into as described in Section 8.2 (Transfers of Data Out of the EEA).

6. Impact Assessments and Consultations

Customer agrees that TimeTec will (taking into account the nature of the processing and the information available to TimeTec) assist Customer in ensuring compliance with any obligations of Customer in respect of data protection impact assessments and prior consultation, including if applicable Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by:

(a) providing the Security Documentation in accordance with Section 5.5.1 (Reviews of Security Documentation); and
(b) providing the information contained in the applicable Agreement including this Data Processing Addendum.

7. Data Subject Rights; Data Export

7.1. Access; Rectification; Restricted Processing; Portability

During the applicable Term, TimeTec will, in a manner consistent with the functionality of the Services, enable Customer to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by TimeTec and to export Customer Data.

7.2. Data Subject Requests

7.2.1. Customer's Responsibility for Requests

During the applicable Term, if TimeTec receives any request from a data subject in relation to Customer Personal Data, TimeTec will advise the data subject to submit his/her request to Customer, and Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

7.2.2. TimeTec's Data Subject Request Assistance

Customer agrees that (taking into account the nature of the processing of Customer Personal Data) TimeTec will assist Customer in fulfilling any obligation to respond to requests by data subjects, including if applicable

Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by complying with the commitments set out in Section 7.1 (Access; Rectification; Restricted Processing; Portability) and Section 7.2.1 (Customer's Responsibility for Requests).

8. Data Transfers

8.1. Data Storage and Processing Facilities

Customer agrees that TimeTec may, subject to Section 8.2 (Transfers of Data Out of the EEA), store and process Customer Data in the United States, Malaysia and any other country in which TimeTec or any of its Subprocessors maintains facilities.

8.2. Transfers of Data Out of the EEA

8.2.1. TimeTec's Transfer Obligations

If the storage and/or processing of Customer Personal Data (as set out in Section 8.1 (Data Storage and Processing Facilities)) involves transfers of Customer Personal Data out of the EEA and the European Data Protection Legislation applies to the transfers of such data ("Transferred Personal Data"), TimeTec will if requested to do so by Customer, ensure that TimeTec as the data importer of the Transferred Personal Data enters into Standard Contractual Clauses with Customer as the data exporter of such data, and that the transfers are made in accordance with such Standard Contractual Clauses.

8.2.2 Customer's Transfer Obligations

In respect of Transferred Personal Data, Customer agrees that if under the European Data Protection Legislation TimeTec reasonably requires Customer to enter into Standard Contractual Clauses in respect of such transfers, Customer will do so.

8.3. Data Storage Information

Information about the locations of TimeTec's data storage for applicable Services is available (and may be updated by TimeTec from time to time) at:

1. https://www.timeteccloud.com/privacypolicy, or
2. https://www.i-neighbour.com/privacy_policy.

8.4 Disclosure of Confidential Information Containing Personal Data

If Customer has entered into Standard Contractual Clauses as described in Section 8.2 (Transfers of Data Out of the EEA), TimeTec will, notwithstanding any term to the contrary in the applicable Agreement, ensure that any disclosure of Customer's Confidential Information containing personal data, and any notifications relating to any such disclosures, will be made in accordance with such Standard Contractual Clauses.

9. Subprocessors

9.1. Consent to Subprocessor Engagement

Customer specifically authorizes the engagement of TimeTec's Affiliates as Subprocessors. In addition, TimeTec and TimeTec's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services ("Third Party Subprocessors"). If Customer has entered into Standard Contractual Clauses as described in Section 8.2 (Transfers of Data Out of the EEA), the above authorizations will constitute Customer's prior written consent to the subcontracting by TimeTec of the processing of Customer Data if such consent is required under the Standard Contractual Clauses.

9.2. Information about Subprocessors

Information about Subprocessors, including their locations, is stated as below:

www.timeteccloud.com/subprocessors

9.3. Requirements for Subprocessor Engagement

When engaging any Subprocessor, TimeTec will:

(a) ensure via a written contract that:

(i) the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the applicable Agreement (including this Data Processing Addendum) and any Standard Contractual Clauses entered into by TimeTec as described in Section 8.2 (Transfers of Data Out of the EEA); and

(ii) if the GDPR applies to the processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR, as described in this Data Processing Addendum, are imposed on the Subprocessor; and

(b) remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

9.4. Opportunity to Object to Subprocessor Changes

(a) When any new Third Party Subprocessor is engaged during the applicable Term, TimeTec will, at least 30 days before the new Third Party Subprocessor processes any Customer Data, inform Customer of the engagement (including the name and location of the relevant subprocessor and the activities it will perform) by sending an email to the Notification Email Address.

(b) Customer may object to any new Third Party Subprocessor by terminating the applicable Agreement immediately upon written notice to TimeTec, on condition that Customer provides such notice within 90 days of being informed of the engagement of the subprocessor as described in Section 9.4(a). This termination right is Customer's sole and exclusive remedy if Customer objects to any new Third Party Subprocessor.

10. Liability

10.1. Liability Cap

If Standard Contractual Clauses have been entered into as described in Section 8.2 (Transfers of Data Out of the EEA), the total combined liability of either party and its Affiliates towards the other party and its Affiliates under or in connection with the applicable Agreement and such Standard Contractual Clauses combined will be limited to the Agreed Liability Cap for the relevant party, subject to Section 10.2 (Liability Cap Exclusions).

10.2. Liability Cap Exclusions

Nothing in Section 10.1 (Liability Cap) will affect the remaining terms of the applicable Agreement relating to liability (including any specific exclusions from any limitation of liability).

11. Third Party Beneficiary

Notwithstanding anything to the contrary in the applicable Agreement, where TimeTec is not a party to such Agreement, TimeTec will be a third party beneficiary of Section 5.5 (Reviews and Audits of Compliance), Section 9.1 (Consent to Subprocessor Engagement) and Section 10 (Liability) of this Data Processing Amendment.

12. Effect of Addendum

To the extent of any conflict or inconsistency between the terms of this Data Processing Addendum and the remainder of the applicable Agreement, the terms of this Data Processing Addendum will govern. Subject to the amendments in this Data Processing Addendum, such Agreement remains in full force and effect.

ATTACHMENT 1

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

[FOR CUSTOMER TO COMPLETE]

Name of the data exporting organisation:

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation

(the data exporter)

And

Name of the data importing organisation: TimeTec Cloud Sdn. Bhd.

Address: No. 6, 8 & 10, Jalan BK 3/2, Bandar Kinrara 47180 Puchong, Selangor, Malaysia

Tel.: +603 - 8070 9933 ; fax: +603 - 8070 9988 ; e-mail: info@timeteccloud.com

Other information needed to identify the organisation: Not applicable

(the data importer)

each a ‘party’; together ‘the parties’,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in 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;

(b) ‘the data exporter’ means the controller who transfers the personal data;

(c) ‘the data importer’ means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses 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;

(d) ‘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 his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) ‘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;

(f) ‘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.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 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. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 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 the Clauses.

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.

Clause 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 the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(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 supervisory authority 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 the Clauses, with the exception of Appendix 2, 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 the Clauses, unless the Clauses 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 subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 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 the Clauses; 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 the Clauses, 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 Appendix 2 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 supervisory authority 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 the Clauses 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 supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 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;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

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.

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 his 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 of 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.

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 the Clauses 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 the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, 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 supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

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.

Clause 8

Cooperation with supervisory authorities

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

2. The parties agree that the supervisory authority 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.

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).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

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

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, 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 the Clauses. 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.

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 the Clauses.

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.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses 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 supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

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.

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

[FOR CUSTOMER TO COMPLETE AND SIGN]

On behalf of the data exporter:

Name (written out in full): ……………………………………………….

Position: ……………………………………………….

Address: ……………………………………………….

Other information necessary in order for the contract to be binding (if any):

Signature: ………………………………………………. (stamp of organisation)

On behalf of the data importer:

Name (written out in full): Teh Hon Seng

Position: Chief Executive Officer

Address: No. 6, 8 & 10, Jalan BK3/2, Bandar Kinrara, 47180 Puchong, Selangor, Malaysia

Other information necessary in order for the contract to be binding (if any):

TIMETEC CLOUD SDN BHD
timeTec
★ 832542 - W ★

Signature: ………………………………………………………….………. (stamp of organisation)

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses 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 Appendix

Data exporter
The Data Exporter is the entity identified as “Customer” in the Addendum.

Data importer
The Data Importer is TimeTec Cloud Sdn. Bhd., a provider of workforce, security management and smart community solutions.

Data subjects
The Data Exporter’s Users (may include, but is not limited to Data Exporter's employees, business partners, vendors, customers, freelancers, contact persons, community members, visitors, guests and any other Users or individuals added into the account).

Categories of data
Personal Data transferred may include, but is not limited to name, user ID, employee ID, contact information (email address, phone, physical business address), employment details (company, job title, department), personal identification details (NRIC or passport number), vehicle license plate number, video camera images and other data added into the account in Customer's sole discretion.

Special categories of data (if appropriate)
Not applicable, unless Data Exporter configures the service to capture such data. For instance, may apply to those using FingerTec fingerprint terminals. Data Exporter may opt to store Fingerprint templates in the server. May also apply to video camera images if it involves processing of biometric data for the purpose of uniquely identifying a natural person (e.g. use of the imagery for facial recognition)

Processing operations
The receipt and storage of Personal Data in the performance of the Services during the Term of the Agreement.

[FOR CUSTOMER TO COMPLETE AND SIGN]

DATA EXPORTER

Name: ……………………………………….

Authorised Signature ……………………………………….

DATA IMPORTER

Name: Teh Hon Seng

Authorised Signature ……………………………………….

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses 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 Clauses 4(d) and 5(c) (or document/legislation attached):

1. General Controls

The following technical and organizational measures will be implemented:

(a) deny unauthorised persons access to data-processing equipment used for processing Personal Data (equipment access control);

(b) prevent the unauthorised reading, copying, modification or removal of data media containing Personal Data (data media control);

(c) prevent the unauthorised input of Personal Data and the unauthorised inspection, modification or deletion of stored Personal Data (storage control);

(d) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment used to process Personal Data (user control);

(e) ensure that persons authorised to use an automated data-processing system only have access to the Personal Data covered by their access authorisation (data access control);

(f) ensure that it is possible to verify and establish to which individuals Personal Data have been or may be transmitted or made available using data communication equipment (communication control);

(g) ensure that it is subsequently possible to verify and establish which Personal Data have been put into automated data-processing systems and when and by whom the input was made (input control);

(h) prevent the unauthorised reading, copying, modification or deletion of Personal Data during transfers of those data or during transportation of data media (transport control);

(i) ensure that installed systems used to process Personal Data may, in case of interruption, be restored (recovery);

(j) ensure that the functions of the system used to process Personal Data perform, that the appearance of faults in the functions is reported (reliability) and to prevent stored Personal Data from corruption by means of a malfunctioning of the system (integrity).

2. Personnel

TimeTec shall take reasonable steps to ensure that no person shall be appointed by TimeTec to process Personal Data unless that person:

(a) is competent and qualified to perform the specific tasks assigned to him by TimeTec;

(b) has been authorised by TimeTec; and

(c) has been instructed by TimeTec in the requirements relevant to the performance of the obligations of TimeTec under these Clauses, in particular the limited purpose of the data processing.

3. Copy Control

TimeTec shall not make copies of Personal Data, provided, however, that TimeTec may retain copies of Personal Data provided to it for backup and archive purposes.

4. Security Controls

The Service includes a variety of configurable security controls that allow the Customer to tailor the security of the Service for its own use. These controls include:

- Unique User identifiers (User IDs) to ensure that activities can be attributed to the responsible individual.
- Controls to revoke access after several consecutive failed login attempts.
- The ability to specify the lockout time period.
- Controls to ensure generated initial passwords must be reset on first use.
- Controls to terminate a User session after a period of inactivity.
- Password length controls.
- Password complexity requirements (requires letters and numbers).

5. Security Procedures, Policies and Logging

The Services are operated in accordance with the following procedures to enhance security:

- User passwords are stored using a one-way hashing algorithm (MD5) and are secured via security token using SHA256.
- Some of user access log entries will be maintained, containing date, time, User ID, URL executed or entity ID operated on, operation performed (viewed, edited, etc.)
- If there is suspicion of inappropriate access, TimeTec or its Sub-processor can provide Customer log entry records to assist in forensic analysis. This service will be provided to Customer on a time and materials basis.
- Passwords are not logged under any circumstances.
- Certain administrative changes to the Services are tracked in an area known as “History” or “Audit Trail” and are available for viewing by Customer’s system administrator.
- User can request to reset password. An email will be sent to the user’s email address to allow user to create a new password for his/her account.

6. User Authentication

Access to the Services requires a valid User ID and password combination, which are encrypted via SSL while in transmission. Following a successful authentication, a random session ID is generated and stored in the user’s browser to preserve and track session state.

7. Security Logs

TimeTec shall ensure that all TimeTec or Sub-processor systems used to store Customer Data, including operating systems, log information or a centralised syslog server.

8. Incident Management

TimeTec maintains security incident management policies and procedures. TimeTec will promptly notify Customer in the event TimeTec becomes aware of an actual or reasonably suspected unauthorised disclosure of Personal Data.

9. Physical Security

All TimeTec services is using Amazon Web services. The data center control can be located at: https://aws.amazon.com/compliance/data-center/controls/

10. Reliability and Backup

All networking components, SSL accelerators, load balancers, Web servers and application servers that are part of the TimeTeccloud.com platform are configured in a redundant configuration. All Personal Data is stored on a primary database server that is clustered with a backup database server for redundancy. All Personal Data is stored on carrier-class disk storage using multiple data paths.

11. Disaster Recovery

TimeTec will ensure that the systems where Customer Data is stored have a disaster recovery facility that is geographically remote from its primary data centre, along with required hardware, software, and Internet connectivity, in the event production facilities at the primary data centre were to be rendered unavailable. TimeTec will ensure that its Sub-processor that stores Customer Data has disaster recovery plans in place and tests them at least once per year.

12. Viruses

The Services will not introduce any viruses to Customer's systems; however, the Services do not scan for viruses that could be included in attachments or other Personal Data uploaded into the Services by Customer. Any such uploaded attachments will not be executed in the Services and therefore will not damage or compromise the Service.

13. Data Encryption

The Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Services, including 256-bit TLS Certificates and 2048-bit RSA public keys at a minimum.

14. System Changes and Enhancements

TimeTec plans to enhance and maintain the Services during the term of the Agreement. Security controls, procedures, policies and features may change or be added. TimeTec will provide security controls that deliver a level of security protection that is not materially lower than that provided as of the Effective Date.

Attachment 2

Subject Matter: TimeTec’s provision of the Services and related technical support to Customer.

Duration of the Processing: The applicable Term plus the period from expiry of such Term until deletion of all Customer Data by TimeTec in accordance with the Data Processing Addendum.

Nature and Purpose of the Processing: TimeTec will process Customer Personal Data submitted, stored, sent or received by Customer, its Affiliates or End Users via the Services for the purposes of providing the Services and related technical support to Customer in accordance with the Data Processing Addendum.

Categories of Data: Name, user ID, employee ID, contact information (email address, phone, physical business address), employment details (company, job title, department), personal identification details (NRIC or passport number), vehicle license plate number, video camera images and other data added into the account in Customer's sole discretion.

Data Subjects: Any individual whose personal data is submitted by Customer to the Services. This may include, but is not limited to Customer's employees, business partners, vendors, customers, freelancers, contact persons, community members, visitors, guests and any other Users or individuals added into Customer's account or authorized by Customer to use the Services.