Trustwave Data Processing Agreement

This Data Processing Agreement ("**DPA**") forms part of the Services Agreement (as defined below) between Trustwave and Client (together, the "**Parties**"). This DPA applies solely where Trustwave processes Personal Data on behalf of the Client in connection with the Services Agreement.

1 Definitions

The terms used in this DPA will have the meanings set forth in this DPA or as defined by applicable Data Protection Laws. Capitalized terms not otherwise defined herein or defined by applicable Data Protection Laws will have the meaning given to them in the Services Agreement. The following terms have the meanings set forth below:

1.1 "**Client**" means the client that is party to the Services Agreement.

1.2 "**Personal Data**" means any personal data including business contact information, name, business address, business telephone and or email, provided by or on behalf of Client to Trustwave, any of its subcontractors or affiliates, in connection with the Services Agreement.

1.3 "**Data Protection Laws**" means all data protection laws applicable to the Parties, as amended from time to time, including, but not limited to (a) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and any binding regulations promulgated thereunder ("**CCPA**"); (b) the EU General Data Protection Regulation 2016/679, including the applicable implementing legislation of each Member State ("**EU GDPR**"); (c) the UK Data Protection Act 2018 and the UK General Data Protection Regulation as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) ("UK GDPR" and together with the EU GDPR, the "**GDPR**"); (d) the Swiss Federal Act on Data Protection of 19 June 1992; (e) any other applicable law with respect to any Personal Data, including any comprehensive United States state privacy laws; and (f) any other data protection law and any guidance or statutory codes of practice issued by any relevant regulatory or supervisory authority.

1.4 "**Member State**" means a country belonging to the European Union or to the European Economic Area ("**EEA**").

1.5 "**Services**" means the services as described in the Services Agreement or any related order form or statement of work.

1.6 "**Services Agreement**" means the Services Agreement entered into by the Parties for the purpose of providing the Services.

1.7 "**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses for the transfer of personal data to third countries, Controller-to-Processor module, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, and implemented by the European Commission decision 2021/914, dated 4 June 2021.

1.8 "**UK Addendum**" means the transfer tool to comply with Article 46 of the UK GDPR for making restricted transfers via an addendum to the European Commission's SCCs for international data transfers.

1.9 "**Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data processed which affects the Personal Data covered by this DPA.

1.10 "**Trustwave**" will refer to the Trustwave entity applicable to Client's location.

1.11 "**UK**" means the United Kingdom.

2 Client Processing Details and Responsibilities

2.1 Roles. The Parties agree to comply with their respective obligations under applicable Data Protection Laws. Client engages Trustwave as a “processor” or “service provider” acting on behalf of Client as stipulated under applicable Data Protection Laws. The Parties agree and acknowledge that Client will be acting as a data controller in respect of the Personal Data processed for the purposes of this DPA.

2.2 Processing. The subject matter, nature, purpose, and duration of the processing, as well as the types of Personal Data collected and categories of data subjects, are described in Annex I of this DPA. Client agrees that the processing activities relating to Personal Data, as specified in the Services Agreement and this DPA, are lawful, fair, and transparent in relation to the data subjects, as set out in Annexes I and II to this DPA. The subject matter of the processing is performance of the Services under the Services Agreement, and the duration of the processing will be for the term of the Services Agreement.

2.3 Privacy Policy. Trustwave may collect Personal Data directly from Client, Client’s end users, or Client’s relevant personnel, and also during Trustwave’s ongoing relationship with Client, Client’s end users, or relevant personnel. Trustwave may use it to supply products and services to Client, and for the other purposes described in Trustwave’s privacy policy, which can be found at https://www.trustwave.com/en-us/legal-documents/privacy-policy/. Without it, Trustwave may not be able to supply products or services in accordance with the Services Agreement. Client agrees that Trustwave may access, share, transfer or store such Personal Data within Trustwave companies and with other service providers and partners for these purposes.

3 Instructions

3.1 Permitted Processing. Trustwave will process Personal Data (including the transfer of Personal Data) only in accordance with Client´s instructions and to perform its obligations under the Services Agreement and this DPA. Trustwave may also process Personal Data where required to do so by applicable law, in which case Trustwave will notify Client of this requirement prior to processing unless the applicable law prohibits Trustwave from doing so.

3.2 Further Instruction. This DPA, the Services Agreement, the SCCs, and the UK Addendum, where applicable, are Client's full instructions to Trustwave for the processing of Personal Data. Any further instructions that go beyond the instructions contained in this DPA, the Services Agreement, the SCCs, or the UK Addendum, where applicable, must be within the subject matter of this DPA, the Services Agreement, the SCCs, and the UK Addendum, where applicable. If the implementation of such further instruction results in costs for Trustwave, Trustwave will inform Client about such costs with an explanation of the costs before implementing the instruction. Only after Client's confirmation to bear such costs for the implementation of the instruction, Trustwave is required to implement such further instruction. Client will give further instructions generally in writing, unless the urgency or other specific circumstances require another (e.g., oral, electronic) form. Instructions in another form than in writing will be confirmed by Client in writing without undue delay. Trustwave may refuse further instructions in case such are technically or commercially not feasible.

3.3 Challenged Instruction. Trustwave will promptly inform Client if, in its opinion, an instruction from Client infringes applicable Data Protection Laws ("**Challenged Instruction**"). In such an event, Trustwave is not obliged to follow the Challenged Instruction.

4 Client Responsibilities

Client will have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired Personal Data. Client represents and warrants that: (a) it has provided, and will continue to provide, all notices and has obtained, and will continue to obtain, all consents, permissions and rights necessary under applicable laws, including Data Protection Laws, for Trustwave to lawfully process Personal Data for the purposes contemplated by the Services Agreement (including this DPA); (b) it has complied with all applicable laws, including Data Protection Laws in the collection and provision to Trustwave of such Personal Data; and (c) it will ensure its processing instructions comply with applicable laws (including Data Protection Laws) and that the processing of Personal Data by Trustwave in accordance with Client’s instructions will not cause Trustwave to be in breach of applicable Data Protection Laws. Client shall indemnify Trustwave from all claims and losses in connection with Client’s breach of this Section 4 and breach of applicable Data Protection Laws.

5 Trustwave Responsibilities

With respect to the Personal Data, Trustwave will:

5.1 ensure that any of its personnel who process Personal Data on behalf of Client have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.2 implement appropriate technical and organizational measures as specified in Annex II to this DPA to protect Personal Data against unauthorized or unlawful processing and accidental destruction or loss, and Client confirms that such are appropriate for its use of the services under the Services Agreement. Trustwave may amend the technical and organizational measures from time to time provided that the amended technical and organizational measures are no less protective than those set out in Annex II to this DPA.

5.3 assist Client through the available technical and organizational measures set forth in Annexes I and II to this DPA, insofar as this is possible, with Client's obligations to respond to requests relating to the exercise of data subject rights under Data Protection Laws, taking into account the nature of the processing and the information available to Trustwave. To the extent the technical and organizational measures specified in Annexes I and II to this DPA or the set-up of the services under the Services Agreement require changes or amendments, Trustwave will advise Client on the costs to implement such additional or amended technical and organizational measures. Once Client has confirmed it will bear such costs, Trustwave will implement such additional or amended technical and organizational measures to assist Client to respond to data subject's requests. Client is obliged to determine whether or not a data subject has a right to exercise any such data subject rights and to give instructions to Trustwave to what extent assistance is required.

5.4 notify Client without undue delay after Trustwave becomes aware of a Security Breach as defined herein or by Data Protection Laws relating to the services provided by Trustwave at Trustwave or a sub-processor. In case of a Security Breach, Trustwave will reasonably assist Client with Client's obligation under Data Protection Laws to inform the data subjects and the supervisory authorities, as applicable, by providing relevant information, taking into account the nature of the processing and the information available to Trustwave.

5.5 provide reasonable assistance to Client (if required by Client) with respect to (a) data protection impact assessments; and (b) prior consultations with applicable regulatory and supervisory authorities to the extent related to the Services provided by Trustwave to Client under the Services Agreement and this DPA, taking into account the nature of the processing and the information available to Trustwave.

5.6 make available to Client information to support Client with respect to its obligation to demonstrate compliance with the obligations in this DPA and applicable Data Protection Laws, in particular with respect to the technical and organizational measures and allow for and contribute to audits, including inspections conducted by Client or another auditor mandated by Client.

5.7 The Parties agree that the aforementioned information obligation is met by providing Client - upon Client's request and subject to a confidentiality agreement between Client and Trustwave to its reasonable satisfaction - with a copy of an annual audit report based on (a) a SOC2 Type 2 Report, (b) a PCI-DSS Attestation of Compliance (AOC) for Products and Core Infrastructure or (c) an ISO 27001 Certificate (covering inter alia the principles security, system availability, and confidentiality) or with similar audit certificates created by a third party ("**Audit Report**").

5.8 To the extent Client's audit requirements may not reasonably be satisfied through the Audit Report, or if additional audit activities are legally required, Client may request inspections conducted by Client or another auditor mandated by Client subject to the execution by such other auditor of a confidentiality agreement with Trustwave to its reasonable satisfaction ("**On-Site Audit**"). Such On-Site Audit is subject to the following conditions: (v) On-Site Audits are limited to the extent processing facilities and personnel of Trustwave are involved in the processing activities covered by this DPA; and (w) On-Site Audits occur not more often than once annually or as required by Data Protection Laws and (x) should be performed during regular business hours, solely insubstantially disrupting Trustwave's business operations and in accordance with Trustwave's security policies, and after at least fifteen (15) business days prior written notice; (y) audits are restricted to those portions of information and any logically separated or entirely dedicated systems and technology used for the processing of Personal Data; and (z) all costs associated with an On-Site Audit will be borne by Client. Client is obliged to create an audit report summarizing the findings and observations of the On-Site Audit ("**On-Site Audit Report**"). On-Site Audit Reports as well as Audit Reports are confidential information of Trustwave and will not be disclosed to third parties unless required by Data Protection Laws, any data protection supervisory authority or subject to Trustwave's prior consent.

5.9 transfer Personal Data only to a country outside the EEA which is approved by the European Commission as providing an adequate level of protection for personal data, or if the country outside the EEA does not ensure an adequate level of data protection, Trustwave will transfer Personal Data pursuant to the SCCs (as per Clause 7 below), or other appropriate legal data transfer mechanisms.

5.10 transfer Personal Data only to a country outside the UK which is approved by the UK ICO as providing an adequate level of protection for personal data, or if the country outside the UK does not ensure an adequate level of data protection, Trustwave will transfer Personal Data pursuant to the UK Addendum (as per Clause 7 below), or other appropriate legal data transfer mechanisms.

5.11 not disclose Personal Data to any third party save as permitted by this DPA, as required by applicable law, or as subsequently directed by Client, and in any event in accordance with the SCCs and the UK Addendum where applicable.

5.12 in accordance with the CCPA, not (a) sell or share (as such terms are defined under the CCPA) Personal Data; (b) retain, use, or disclose Personal Data for any purpose other than for the specific purpose of performing the Services, including retaining, using, or disclosing Personal Data for a commercial purpose other than providing the Services; (c) retain, use, or disclose Personal Data outside of the direct business relationship between Trustwave and Client; or (d) combine the Personal Data with any other personal data, except as specifically instructed by Client in writing.

5.13 notify Client without undue delay in the event Trustwave determines that it can no longer meet its obligations under applicable Data Protection Laws. Upon prior notice to Trustwave, Client may take reasonable and appropriate steps to stop and remediate Trustwave's unauthorized use of Personal Data.

5.14 on expiry or termination of this DPA, upon receipt of a written request of Client, either delete or return to Client such Personal Data which are processed by Trustwave on behalf of Client under this DPA, and to not further process the Personal Data, after the end of the provision of Services, and delete existing copies, unless applicable law requires Trustwave to retain Personal Data.

6 Subprocessors

Client authorizes Trustwave to engage sub-processors to process Personal Data and authorizes the use of sub-processors engaged by Trustwave for the provision of the services under the Services Agreement and this DPA. Client may review Trustwave's current list of sub-processors here: https://www.trustwave.com/en-us/legal-documents/. Trustwave will provide Client prior notice of any additional or replacement sub-processors via an email notifying Client to view the updated sub-processor list at the above-mentioned webpage. After being notified, Client must notify Trustwave within fourteen (14) business days of any reasonable objection Client has to such sub-processors. In the event Client provides a reasonable objection, Trustwave will use commercially reasonable efforts to make a change in processing under the Services Agreement to avoid processing of Personal Data by such sub-processors. If Trustwave is unable to make available such change within a reasonable period, which will not exceed thirty (30) days, Client may terminate the Services provided under the Services Agreement in respect only to those services which cannot be provided by Trustwave without the use of the objected-to sub-processor, by providing written notice to Trustwave. Trustwave will ensure that any sub-processors to whom it transfers Personal Data enter into written agreements with Trustwave requiring that the sub-processor abide by terms no less protective than this DPA.

7 International Data Transfers

7.1 SCCs. To the extent that Trustwave processes Personal Data protected by GDPR in a country outside of the EEA that is not recognized as providing an adequate level of protection for Personal Data, the Parties agree to enter into the appropriate SCCs, the terms of which are incorporated into this DPA. In furtherance of the foregoing, the Parties agree that:

7.1.1 Client will act as the data exporter, and Trustwave will act as the data importer under the SCCs;

7.1.2 for purposes of Annex I to the SCCs, the categories of data subjects, data, special categories of data (if appropriate), and the processing operations will be as set out in Annex I of this DPA;

7.1.3 for purposes of Annex II to the SCCs, the technical and organizational measures will be as set out in Annex II of this DPA;

7.1.4 The optional docking clause in Clause 7 of the SCCs will be included;

7.1.5 the audits described in Clause 8.9 of the SCCs will be performed in accordance with Section 5.6 of this DPA;

7.1.6 Section 6 of this DPA will constitute the procedures for Trustwave to request general authorization for sub-processors under Clause 9(a)(Option 2) of the SCCs;

7.1.7 the optional language in Section 11(a) of the SCCs will not be included;

7.1.8 for Clause 13(a) of the SCCs, the supervisory authority will be as set forth in Section C of Annex I.

7.1.9 Option 1 of Clause 17 of the SCCs will apply, and the SCCs will be governed by the law of Germany; and

7.1.10 any dispute arising from the SCCs will be resolved by the courts of Frankfurt am Main.

7.2 UK Addendum. To the extent that Trustwave processes Personal Data protected by UK GDPR in a country outside of the UK that is not recognized as providing an adequate level of protection for Personal Data, the Parties agree to enter into the UK Addendum, the terms of which are hereby incorporated into this DPA. In furtherance of the foregoing, the Parties agree that:

7.2.1 Table 1: Reference to Table 1 will be satisfied by the information in Section A of Annex I.

7.2.2 Table 2: For Table 2, the version of the Approved EU SCCs will be the SCCs, Controller-to-Processor module.

7.2.3 Table 3: Reference to Table 3 will be satisfied by the information in Annexes I and II.

7.2.4 Table 4: For Table 4, the Importer and Exporter will have the rights outlined in Section 19 of the UK Addendum.

7.3 Conflict. If and to the extent there should be contradictions or inconsistencies between the remainder of this DPA and the Annexes I and II to this DPA, the provisions of the Annexes I and II to this DPA will prevail. For the avoidance of doubt, provisions of the remainder of this DPA that merely go beyond the Annexes I and II to this DPA without contradicting its terms will remain valid.

8 Governing Law and Jurisdiction

This DPA is governed by the law specified in the Services Agreement and subject to the jurisdiction of the courts specified in that agreement.

9 Execution

This DPA is deemed agreed by the Parties, and comes into effect on the Effective Date, which is the earlier of (a) the date that the Services Agreement is signed by Client; and (b) thirty (30) calendar days after the date on which this DPA is received by Client ("**Reception Date**"), except where Trustwave receives in writing Client's objections to the terms of this DPA within thirty (30) calendar days of the Reception Date. If Client objects to the terms of this DPA in full or in part, the Parties will promptly and in good faith resolve Client's objections and agree on a form of this DPA acceptable to the Parties, in which case the Effective Date will be the date on which the agreed form of the DPA is signed by the Parties.

10 Claims

The Parties agree that Trustwave's liability with respect to any claims brought under, or in connection with, this DPA, will be subject to the exclusions and limitations of liability set forth in the Services Agreement.

11 Amendments

The Parties acknowledge and agree that, to the extent the Services contemplate the processing of Personal Data that is subject to Data Protection Laws that require additional terms in this DPA, the Parties will enter into an amendment to this DPA that addresses such additional terms.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Client, as defined in the Services Agreement

Address: As set out in the Services Agreement

Contact person's name, position, and contact details: As set out in the Services Agreement

Activities relevant to the data transferred under the DPA: The provision of Trustwave cybersecurity services, including managed security, technologies, and consulting agreements

Signature and date: As set out in the Services Agreement

Role (controller/processor): controller

Data importers:

1. Trustwave Holdings, Inc.

Address: 251 Little Falls Drive, Wilmington, DE 19808

2. TWH Australia Pty Ltd.

Address: C/o Intertrust Australia Pty Ltd, Suite 2, Level 25, 100 Miller Street, North Sydney NSW 2000

3. Trustwave Philippines, Inc.

Address: Armstrong Corporate Centre, 7th Floor, 134 Salcedo Village, H.V. Dela Costa, Makati City, The Philippines

4. Trustwave Pte.

Address: #23-01 BNI Tower, 30 Raffles Place, Singapore 048622

For importers 1 through 4 above:

Contact person's name, position, and contact details: Joel Smith, Chief Administrative Office, General Counsel, & DPO; dataprotection@trustwave.com

Activities relevant to the data transferred under the DPA: The provision of Trustwave cybersecurity services, including managed security, technologies, and consulting agreements

Signature and date: As set out in the Services Agreement

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Client staff, Client's company or company-related website users, or Client's end customers.

Categories of personal data transferred

Full name, business contact details (e.g., work email address, work phone number), IP address, log-in details.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Personal Data transferred should not contain sensitive data, unless otherwise provided by the Data Exporter.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

Personal Data is transferred on a continuous basis for the term of the Services Agreement.

Nature of the processing

Personal Data may be processed by Trustwave while providing cybersecurity services to Client, as defined in the Services Agreement. Trustwave may store, access, analyze, or transfer Personal Data as part of its processing activities as defined in the Services Agreement.

Purpose(s) of the data transfer and further processing

Data Importer processes Personal Data in accordance with the instructions of the Data Exporter as set forth in the Services Agreement and the DPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal Data will be retained for so long as required to provide the services under the Services Agreement, unless otherwise agreed in writing.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The sub-processors will process Personal Data as necessary to provide the services pursuant to the respective services agreements with Trustwave. Personal Data will be processed as long as required to provide the services, unless otherwise agreed in writing.

C. COMPETENT SUPERVISORY AUTHORITY

Where the data exporter is established in an EU Member State: the supervisory authority with responsibility for ensuring compliance by the data exporter with GDPR as regards the data transfer will act as competent supervisory authority.

Where the data exporter is not established in an EU Member State but falls within the territorial scope of application of GDPR (i.e., Article 3(2) GDPR) and has appointed a representative in the EU (i.e., Article 27(1) GDPR): the supervisory authority of the Member State in which the representative is established will act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR without however having to appoint a representative in the EU: the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under the SCCs in relation to the offering of goods or services to them, or whose behavior is monitored, are located, will act as competent supervisory authority.

ANNEX II –

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TO ENSURE THE SECURITY OF THE DATA

Physical Access Control

Permanently locked doors and windows

Security locks

Use of special security doors and armored glass

Permanently manned reception (building)

Single access entry control systems

Automated system of access control

ID or chip card readers

Code locks on doors

Monitoring installations (e.g., alarm device, video surveillance)

Logging of visitors

Compulsory wearing of ID cards

Security personnel

Careful selection of cleaning and maintenance personnel

Security Awareness Training

System Access Control

Individual allocation of user rights

Authentication by username and password

Minimum requirements for passwords (i.e., at least eight characters, alphanumeric combinations allowing use of special characters, no acceptance of trivial passwords (e.g., 12345), no acceptance of same characters in arrow)

Password management (storage of password only as hash, blocking of account after three failed log in

attempts, logging of failed log in attempts, presentation of last log in (date, time) to user for self-control; compulsory change of password every three month, no acceptance of same password in a row)

Password request after inactivity

Encryption of data

Virus protection and firewall

Intrusion detection systems

Security Awareness Training

Data Access Control

Access to personal data only on a need-to-know-basis

Development of a role-based authorization concept

Permanent updating of role-based authorization concept

General access rights only for limited number of admins

Logging of access to and copying, modifying and deletion of personal data

Encryption of data

Intrusion detection systems

Secured storage of data carriers

Secure data lines, distribution boxes and sockets

Secure deletion of personal data and destruction of data carriers and recording of deletion and destruction

Transfer Control

Use of VPN tunnels

Encrypted email communication

Content filter for outgoing data

Firewall

Secure transport containers in case of physical transports

Encryption of mobile data carriers (such as USB sticks or external USB hard drives), laptops, tablets and smartphones

Recording of data transfers

Input Control

Logging of entering, modification and removal of personal data in/from the system

Traceability of entering, modification and removal of personal data by logging usernames (not user groups)

Individual allocation of user rights to enter, modify or remove based on a role-based authorization concept

Job Control

Diligent selection of service providers (in particular with respect to IT security)

Conclusion of a commissioned data processing agreement

Written instructions to service provider

Service provider has implemented a data protection contact

Service provider has obligated its employees to comply with data secrecy

Internal audit and continuous review of compliance

Documentation of technical and organizational IT security measures implemented by service provider

Availability Control

Uninterruptible power supply and auxiliary power unit

Backup and recovery systems (such as RAID)

Redundant servers in separate location

Physical backup in separate location

Climate monitoring and control for servers

Fire and smoke detection

Fire extinguishing system

Fire resistant doors

Malware protection

Emergency plan

Separation Control

Physically separated storage on different hardware systems or data carriers

Logical client separation

Defining and attaching processing purposes for data sets

Defining and implementing database access properties

Development of a role-based authorization concept

Separation of test data and live data

Encryption of data sets stored for the same purpose

Separating allocation file from data sets when personal data is alias

Trustwave binds its sub-processors to technical and organizational measures substantially equivalent to those to which Trustwave has committed in this Annex II.