WiseTech Global Data Processing Addendum

CONTENTS

INTRODUCTION

This Data Processing Addendum and its schedules (**DPA**) form part of the agreement between WTG and the relevant counterparty for the delivery of services by WTG (**Services**, **Agreement**). This DPA reflects the Parties' agreement for the Processing of Personal Data and WTG's commitment to secure Personal Data Processing.

TERMS

1 ACCEPTANCE

1.1 This DPA is pre-signed by WTG and is effective on the date it is accepted by Controller (**Effective Date**). Controller accepts this DPA in its own name and on behalf of its Authorised Affiliates by:

(a) signing and accepting the Agreement in which this DPA is incorporated;

(b) signing this DPA;

(c) acceptance of this DPA in a 'click-to-accept' process, such as when creating an organisation account on eRequest; or

(d) continuing to use the Services for ten days after receiving notice from WTG that the DPA applies to the Processing of Controller's Personal Data and that Controller has the option of not accepting the DPA by terminating the Agreement.

1.2 Controller agrees to:

(a) complete and sign the section 'data exporter' in section 1 of Schedule 1; and

(b) return the completed and signed section 1 of Schedule 1 to WTG by email to licensemanagement@wisetechglobal.com within ten days after acceptance under section 1.1.

2 SCOPE OF APPLICATION

2.1 This DPA is an addendum to and forms part of the Agreement if:

(a) the entity accepting this DPA as Controller is party to the Agreement; and

(b) WTG is a Processor for Controller in relation to the Services provided under the Agreement.

2.2 This DPA is not valid or binding if purportedly accepted or signed by an entity that does not have a direct contractual relationship with WTG through being a party to the Agreement.

3 DEFINITIONS

3.1 In this DPA:

Affiliate means any entity controlling, controlled by, or under common control of the subject entity. For the purposes of this definition, 'control' (including in phrases such as 'controlled by' and 'under common control with'), means the possession, directly or indirectly, of the power to direct or exercise a controlling influence on the management or policies of that entity, whether through the ownership of voting securities, by contract or otherwise.

Authorised Affiliate means any of Controller's Affiliates which:

(a) are subject to Data Protection Laws requiring entry into a data processing agreement; and

(b) are permitted to use Services under the Agreement.

Controller means the non-WTG entity party to the Agreement and includes its Authorised Affiliates (unless otherwise stated). The term 'Controller' is also used when a non-WTG entity party to the Agreement or any of its Authorised Affiliates is acting as a processor under Data Protection laws (in which case WTG acts as subprocessor).

Data Protection Laws means all laws and regulations, including all international, national, state and local laws and regulations, including for example those of the EEA and its member states, Switzerland, the UK, Australia, and U.S. laws, including but not limited to the CCPA, and other U.S. and state laws, applicable to the Processing of Personal Data under the DPA.

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

Data Subject Request means any request from a Data Subject to exercise its rights under Data Protection Laws, including a Data Subject's right of access, right to rectification, restriction of Processing, erasure ('right to be forgotten'), data portability, object to the Processing, or its right not to be subject to an automated individual decision making.

EEA means the European Economic Area.

EU means the European Union.

EU SCCs means Standard Contractual Clauses for the transfer of Personal Data to third countries under Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eurlex.europa.eu/eli/dec_impl/2021/914/oj.

eRequest is WTG's customer support ticketing system.

GDPR means the 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 (General Data Protection Regulation).

ICO UK Addendum means the template Addendum B.1.0 issued by the Information Commissioner of the UK and laid before the UK Parliament in accordance with s119A of the UK Data Protection Act 2018 on 2 February 2022, as it is revised from time to time under section 18 of its mandatory clauses.

Information Security Documentation means the documentation available at the WTG information security website available at https://wisetechglobal.com/what-we-do/information-security/.

Party means each of Controller and WTG, and 'Parties' means Controller and WTG collectively.

Personal Data means any information relating to an identified or identifiable natural person, and that is (part of) the data defined in the Agreement as 'Customer Data', 'Your Data' or with a comparable term, provided that this data is electronic data and information submitted by or for Controller to the Services.

Privacy Documentation means the WTG Privacy help centre available at https://wisetechglobal.com/legal/privacy-help-center/.

Processing or **Process** means any operation or set of operations which is performed on the Personal Data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor means the entity that Processes Personal Data on behalf of the Controller.

Subprocessor means any processor engaged by WTG or a member of the WTG Group and any further processors engaged by those processors.

TOMs means the technical and organisational measures for the relevant Service whose description is available on the Privacy Documentation website.

WTG means the WTG entity which is a party to the Agreement.

WTG Group means WTG and its Affiliates engaged in the Processing of Personal Data.

4 DESCRIPTION OF PROCESSING

Details of Processing operations, including categories of Personal Data and the purposes of Processing, are in Schedule 1.

5 PROCESSING ON CONTROLLER'S INSTRUCTIONS

5.1 Controller and WTG agree that Controller is the controller of Personal Data (or similar concept) under Data Protection Laws and WTG is the processor of that data (or similar concept) under Data Protection Laws, except when Controller acts as a processor of Personal Data, in which case WTG is a subprocessor (or similar concept) under Data Protection Laws. In the latter case Controller warrants to WTG that Controller's instructions, including appointment of WTG as a subprocessor, are authorised by the relevant controller (on whose behalf Controller is acting as a processor).

5.2 WTG must Process Personal Data on behalf of and only in accordance with Controller's documented instructions for the following purposes:

(a) Processing in accordance with the Agreement;

(b) Processing initiated by users in their use of the Services, which is consistent with the terms of the Agreement; and

(c) Processing to comply with other documented reasonable instructions provided by Controller (e.g., via email).

5.3 If required by applicable law, WTG will also Process Personal Data without documented instructions from Controller. In such a case, WTG must inform Controller of the legal requirement before Processing, unless the law prohibits this (where the GDPR or UK GDPR applies: on important grounds of public interest).

5.4 WTG must inform Controller if, in WTG's opinion, instructions given by Controller may infringe the GDPR. In this event, or in the event WTG forms the view that any instructions from the Controller may infringe any other Data Protection Laws, WTG has the right to suspend the execution of the corresponding instruction until it has been confirmed or changed by the Controller after review. To this end, the Controller agrees to provide all reasonable assistance and assurances to WTG of the lawfulness of instructions.

6 PROCESSING FOR WTG'S OWN PURPOSES

6.1 Controller authorises WTG to Process Personal Data for WTG's own purposes of general product research and development, including creating new products, services, or components not specific to a given service or customer (together, **Product Development**), provided the output of this Processing does not identify Controller or its users, or any other natural persons, or otherwise reveal confidential information of Controller (**Product Development Processing**).

6.2 For Product Development Processing, WTG will apply principles of data minimisation and must not use or otherwise process Personal Data for:

(a) user profiling;

(b) advertising or similar commercial purposes, or

(c) any other purpose, other than for Product Development as set out in section 6.1.

7 CONTROLLER OBLIGATIONS

7.1 Controller must, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws, including any applicable requirement to provide notice to Data Subjects of the use of WTG as Processor or Subprocessor.

7.2 Controller's instructions for the Processing of Personal Data must comply with Data Protection Laws. Controller is solely responsible for the accuracy, quality, and legality of Personal Data and the means by which Controller acquired Personal Data. Controller represents and warrants that its use of the Services does not violate the rights of any Data Subject, including those that have

opted-out from sales or other disclosures of Personal Data to the extent applicable under Data Protection Laws.

7.3 Unless expressly agreed with WTG for a particular Service, Controller must not, in its use of the Services, Process any Personal Data defined as special categories of personal data or sensitive personal data (or similar concept) under Data Protection Laws (including personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health data, data concerning a natural person's sex life or sexual orientation).

8 DATA SUBJECT RIGHTS

8.1 To the extent legally permitted, WTG must promptly notify Controller of any Data Subject Request WTG receives relating to Controller's Personal Data.

8.2 WTG must not respond substantively to a Data Subject Request itself, unless authorised to do so in writing (with email sufficient) by Controller.

8.3 Considering the nature of the Processing, WTG must assist Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfillment of Controller's obligation to respond to a Data Subject Request under Data Protection Laws.

8.4 To the extent that Controller in its use of the Services does not have the ability to address a Data Subject Request, then on Controller's request, WTG must provide commercially reasonable efforts to assist Controller in responding to the Data Subject Request. This obligation applies only if WTG is legally permitted to do so and the response to the Data Subject Request is required under Data Protection Laws. Unless prohibited by applicable law, Controller must reimburse WTG's costs (including internal costs) in connection with this assistance.

9 SECURITY

9.1 WTG has implemented the TOMs for the relevant Service to ensure the security of the Personal Data. This includes protecting the Personal Data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (**Personal Data Breach**). In assessing the appropriate level of security, the Parties must take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the risks involved for the Data Subjects.

9.2 WTG monitors compliance with the TOMs and can change the TOMs in its free discretion as long as the change does not materially decrease the overall security of the Services, and the security level required under Data Protection Laws is maintained. WTG will publish any material updates to the TOMs for the relevant Service via update notes in the usual course and will have a mechanism for the Customer to subscribe to relevant updates.

9.3 WTG must ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

10 CERTIFICATIONS, INFORMATION REQUESTS AND AUDITS

10.1 WTG must maintain an audit program to help ensure compliance with the obligations in this DPA and must make available to Controller information to demonstrate compliance with the obligations in this DPA, as set out in this section 10.

10.2 WTG has obtained the certifications and audit reports set out in the Information Security Documentation for the relevant Service.

10.3 Subject to 10.4, Controller may, during regular business hours without unreasonably interfering with WTG's business operations, and after a reasonable prior notice, personally audit WTG, or appoint a third-party auditor, who is subject to confidentiality obligations and not acting as a competitor of WTG, to carry out the audit at Controller's sole cost.

10.4 The following requirements apply to audits under clause 10.3:

(a) Controller agrees to audit WTG not more than once per year and only after a reasonable prior notice being not less than 30 days, unless the additional audit is required by a decision of a data protection supervisory authority or a court that is final and binding on Controller, or under Data Protection Laws following a Personal Data Breach at WTG concerning the Personal Data of Controller.

(b) Before the initiation of any on-site audit, Controller and WTG must agree on the scope, timing, and duration of the audit. WTG must, upon request and within a reasonable time, provide Controller with relevant information to assist an audit of the Processing governed by this DPA.

(c) On-site audits will be subject to such safety, workplace and security protocols as reasonably required by WTG to ensure the safety of Controller's and WTG's personnel, security of systems and confidentiality of WTG and WTG customer data.

(d) In deciding on an audit, Controller must consider relevant certifications held or audit reports provided by WTG and as set out in the Information Security Documentation for the relevant Service. If the requested audit scope is addressed in the certification or audit report issued by a qualified third party auditor within the prior twelve months and WTG provides the certification or report to Controller confirming there are no known material changes in the controls audited, then Controller agrees to accept the findings presented in the third party audit report instead of requesting an audit of the same controls covered by the certification or report.

(e) Controller must ensure that the results of the audit report are kept confidential, unless disclosure is required by a data protection supervisory authority, a court or under Data Protection Laws.

(f) Provided that WTG notifies Controller of the costs to be incurred either before the audit takes place or the information is provided, then WTG may charge Controller for the reasonable costs (including costs for internal staff and external contractors) incurred with respect to responding to information requests and assisting with audits.

11 DATA PROTECTION IMPACT ASSESSMENTS

On request and at the expense of Controller, WTG must provide Controller with reasonable cooperation and assistance to carry out a data protection impact assessment or to consult a data protection supervisory authority in advance in connection with Controller's use of the Services, but only to the extent:

(a) necessary to comply with Controller's obligations under Data Protection Laws;

(b) Controller does not otherwise have access to the relevant information (including as part of the Privacy Documentation provided by WTG); and

(c) WTG holds relevant information.

12 INCIDENT MANAGEMENT AND NOTIFICATIONS

WTG must notify Controller without undue delay after becoming aware of a Personal Data Breach. Subject to the nature of the Processing, and the information available to WTG, the notification must include information relevant to reasonably assist Controller in ensuring compliance with Controller's own notification obligations under Data Protection Laws. To the extent it is not possible to provide all relevant information at the same time, WTG may provide the information in phases without further undue delay. Controller agrees to coordinate with WTG on the content of any intended public statements or required notices to affected Data Subjects or relevant authorities regarding the Personal Data Breach.

13 SUBPROCESSORS

13.1 Controller consents to and generally authorises the engagement of Subprocessors by WTG or WTG Affiliates. A current list of Subprocessors engaged in Processing Personal Data for the performance of each applicable Service – which may be updated by WTG from time to time – can be found on the Privacy Documentation website. WTG or a WTG Affiliate has entered into a written agreement with each Subprocessor containing, in substance, data protection obligations no less protective than those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by the Subprocessor.

13.2 The Privacy Documentation contains a mechanism to subscribe to notifications of new Subprocessors for each applicable Service, and if Controller subscribes, WTG must provide notification of a new Sub-processor to Controller through this mechanism.

13.3 Controller may object to WTG's use of a new Subprocessor by notifying WTG promptly in writing within ten days of receipt of WTG's notice in accordance with the mechanism in section 13.2 above. If Controller objects to a new Subprocessor and that objection is duly substantiated and not unreasonable, then WTG must use reasonable efforts to make available to Controller a change in the Services or, alternatively, recommend a commercially reasonable change to Controller's configuration or use of the Services to avoid Processing of Personal Data by the contested new Subprocessor without unreasonably burdening Controller. If WTG is unable to make the change available within a reasonable period, which must not exceed 30 days, then Controller may terminate the relevant portion(s) of the Services which cannot be provided by WTG without the use of the contested new Subprocessor by providing written notice to WTG.

13.4 No Processing by a Subprocessor releases WTG from its responsibility for its obligations under this DPA, and WTG is liable for the acts and omissions of Subprocessors to the same extent WTG would be liable if performing the services of each Subprocessor directly under the terms of this DPA, subject to the limitations in this DPA (in particular section 15 below) and in the Agreement.

14 AUTHORISED AFFILIATES

14.1 Controller acknowledges and agrees that it enters into this DPA, including if applicable the EU SCCs, adjusted as necessary for transfers from Switzerland and the UK (in form of the ICO UK Addendum), in the name and on behalf of its Authorised Affiliates, thereby establishing a separate DPA, and if applicable separate EU SCCs relationship, between WTG and each Authorised Affiliate subject to the provisions of this section 14. Each Authorised Affiliate agrees to be bound by the obligations of its DPA and, to the extent applicable, the obligations of the EU SCCs incorporated into this DPA. For the avoidance of doubt, an Authorised Affiliate is not entering into a separate Agreement with WTG.

14.2 Controller remains responsible for coordinating all communication with WTG under this DPA and the DPAs of its Authorised Affiliates and is entitled to make and receive any communication in relation to the DPAs of its Authorised Affiliates on their behalf.

14.3 If an Authorised Affiliate enters into a DPA with WTG, then it is entitled to exercise the rights and seek remedies of the Controller under its DPA, subject to the following:

(a) its exercise of rights and remedies is limited to the extent required under Data Protection Laws;

(b) unless Data Protection Laws require the Authorised Affiliate to exercise a right or seek any remedy under its DPA against WTG directly, the Parties agree that:

(i) only the Controller may exercise any right or seek any remedy on behalf of the Authorised Affiliate, and

(ii) Controller must exercise any rights under this DPA and the DPAs of its Authorised Affiliates not separately for each Authorised Affiliate individually, but jointly for itself and all its Authorised Affiliates together (as, for example, in section 14.3(c), below).

(c) The Parties agree that Controller must, when carrying out an audit in accordance with section 10 take all reasonable measures to limit any impact on WTG and Subprocessors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorised Affiliates in one single audit.

(d) Controller represents and warrants that it has been duly authorised by its Authorised Affiliates to enter a separate DPA, and if applicable separate EU SCCs relationship, in the name and on behalf of its Authorised Affiliates.

15 LIMITATION OF LIABILITY

15.1 Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorised Affiliates and WTG, whether in contract, tort or under any other theory of liability, is subject to the limits of liability in the Agreement, and any reference to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

15.2 WTG's and its Affiliates' total liability for all claims from Controller and all of its Authorised Affiliates arising out of or related to the Agreement and all DPAs applies in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Controller and all Authorised Affiliates, and, in particular, does not apply individually and severally to either or both of Controller and any Authorised Affiliate that is a contracting party to any DPA.

15.3 If the Agreement does not include an overall cap on liability, then each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorised Affiliates and WTG, whether in contract, tort or under any other theory of liability, will not exceed the total amount paid by Controller and its Authorised Affiliates for the Services giving rise to the liability in the twelve months preceding the first incident out of which the liability arose.

16 EEA/SWISS/UK INTERNATIONAL TRANSFERS

16.1 In providing the Services, WTG may transfer Controller's or any Authorised Affiliate's Personal Data that is subject to Data Protection Laws of the EEA, Switzerland or the UK, to WTG and Subprocessors outside of the EEA, Switzerland or the UK.

16.2 For data transfers under section 16.1, Controller (on its own behalf and on behalf of its Authorised Affiliates) and WTG agree to be bound by the EU SCCs (Module 2: Transfer Controller to Processor) on acceptance under sections 1.1 and 1.2 of this DPA and adjusted as necessary for transfers from Switzerland and the UK (in form of the ICO UK Addendum). These EU SCCs are deemed incorporated into this DPA in their entirety and apply as further specified in Schedule 2 to this DPA. If the EU SCCs (Module 2: Transfer Controller to Processor) are no longer available or do not authorise an international transfer of Personal Data to WTG, the Controller agrees to cooperate in good faith to enter into any additional agreements or take any other action that may be legally required by either Party to comply with transfer requirements under Data Protection Laws.

16.3 Controller agrees that when WTG engages Subprocessors under this DPA to carry out Processing activities (on behalf of Controller) involving a transfer of Personal Data outside of the EEA, Switzerland or the UK, WTG and the Subprocessor may rely on the EU SCCs (Module 3: Transfer Processor to Processor), adjusted as necessary for transfers from Switzerland and the UK, provided the conditions for the use of those Standard Contractual Clauses are met.

16.4 If there is any conflict or inconsistency between the provisions of the main body of this DPA and the provisions of the EU SCCs (Module 2: Transfer Controller to Processor), adjusted as necessary for transfers from Switzerland and the UK ((in form of the ICO UK Addendum), then the (adjusted) EU SCCs prevail.

17 OTHER COUNTRY-SPECIFIC PROVISIONS

17.1 In providing the Services, WTG may transfer Controller's or any Authorised Affiliate's Personal Data that is subject to the Data Protection Laws of jurisdictions other than the EEA, Switzerland or the UK, to WTG and Subprocessors located outside of those jurisdictions.

17.2 For data transfers under section 17.1 and to address certain jurisdiction-specific Processing requirements, the provisions in Schedule 3 et seqq. form an integral part of this DPA and apply as further specified in those Schedules.

17.3 If there is any conflict or inconsistency between the provisions of the main body of this DPA and the provisions of Schedule 3 et seqq., then the provisions of Schedule 3 et seqq prevail.

18 DURATION AND TERMINATION; RETURN OR DELETION OF PERSONAL DATA

18.1 This DPA becomes effective upon the Effective Date in section 1.1. It terminates automatically on termination of the Agreement or if the Processing under the Agreement is permanently discontinued.

18.2 If this DPA is terminated, then WTG must return to Controller or delete, at Controller's choice, all Personal Data Processed on behalf of Controller, unless applicable law requires storage of the Personal Data. On request of Controller, WTG must confirm compliance with these obligations in writing. If the Controller does not exercise its right of return of Personal Data within 60 calendar days, then WTG may delete the Personal Data of the Controller.

19 MISCELLANEOUS PROVISIONS

19.1 This DPA may be changed or amended as provided for in the Agreement, or otherwise by WTG if required under Data Protection Laws. WTG must notify Controller in advance of any change or amendment. If Controller continues to use the Services for ten days after receiving notice from WTG of a change or amendment to the DPA and has been provided with the option to terminate the Agreement, then the continued use of the Services for ten days is deemed to be acceptance of the change or amendment to the DPA.

19.2 If any provision of this DPA is or becomes invalid, then this does not affect the validity of the remaining terms. The Parties must cooperate in the creation of terms which achieve a legally valid result that is commercially closest to that of the invalid provision. This applies accordingly to the closing of any gaps in the DPA.

19.3 Any WTG obligations arising from statutory provisions or according to a judicial or regulatory decision remain unaffected by this DPA.

19.4 This DPA does not replace any comparable or additional rights relating to Processing of Personal Data of Controller contained in the Agreement. In the event of any conflict or inconsistency between this DPA and the Agreement, this DPA prevails.

19.5 DPA is governed by the same law that governs the Agreement between the Parties, except for the EU SCCs which are governed by the law applicable under Clause 17 of the SCCs and section 14 of Schedule 2 (EEA/Swiss/UK Specific Transfer Provisions) of this DPA as well as, for any data transfers governed by the UK GDPR, section 18 of Schedule 2 (EEA/UK/Swiss Specific Transfer Provisions) of this DPA in connection with section 15(m) of the ICO UK Addendum. Data transfers which are subject to the provisions in Schedule 3 et seqq. are governed by the respective law in the applicable Schedule (if any).

List of Schedules

Schedule 1: Description of Processing
Schedule 2: EEA/Swiss/UK
Schedule 3: U.S.
Schedule 4: PRC
Schedule 5: Taiwan
Schedule 6: Australia
Schedule 7: Brazil
Schedule 8: Turkey

EXECUTION

Signed by Controller:

Controller

Signature

Name

Title

Schedule 1 - Description of Processing

This Schedule 1 includes certain details of the Processing of Personal Data by WTG on behalf of Controller and its Authorised Affiliates.

1 LIST OF PARTIES

Data Exporter(s): Identity and contact details of the data exporter(s) and, if applicable, of its/their data protection officer and/or representative in the European Union

Name: Controller and its Authorised Affiliates

Address:

Activities relevant to the data transferred under these clauses: Performance of the Services under the Agreement.

Name, signature and date:

_____

Role (controller/processor): Controller and its Authorised Affiliates are each acting as a Data Controller.

Data Importer(s):

Name: WTG

Dr. Sebastian Kraska

Rechtsanwalt, Diplom-Kaufmann

IITR Datenschutz GmbH, Eschenrieder Str. 62c, 82194 Gröbenzell

Telefon: +49 89 189 1736-0

E-Mail: skraska@iitr.de

Activities relevant to the data transferred under these clauses: Performance of the Services under the Agreement.

Name, signature and date:

_____

Maree Isaacs, Head of License Management and Authorised Officer for WiseTech Global Limited and its Affiliates

Role (controller/processor): WTG is acting as a Data Processor.

2 DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Subject to use and Processing restrictions in the Agreement and this DPA, Controller may submit Personal Data to the Services, the extent of which is determined and controlled by Controller in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customers;
- Customer's customers;
- Potential Customers;
- Subscribers;
- Employees;
- Suppliers;
- Authorised Agents; and
- Contact Persons.

Categories of personal data transferred

Subject to use and Processing restrictions in the Agreement and this DPA, Controller may submit Personal Data to the Services, the extent of which is determined and controlled by Controller in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- Personal Master Data (Key Personal Data);
- Contact Data;
- Key Contract Data (Contractual/Legal Relationships, Contractual or Product Interest);
- Customer History;
- Contract Billing and Payments Data; and
- Disclosed Information (from third parties, e.g. Credit Reference Agencies or from Public Directories.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, including for example 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.

Controller must not submit any Personal Data to the Services that are defined as special categories of personal data or sensitive personal data (or similar concept) under Data Protection Laws (including personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health data, data concerning a natural person's sex life or sexual orientation), unless this has been expressly agreed with WTG for a particular Service. If agreed with WTG, the specifically applicable technical and organisational measures are set out as part of the description of the TOMs for the relevant Service.

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

Personal Data is transferred on an ongoing and continuous basis depending on the use of the Services by Controller.

Nature of the Processing

The nature of the Processing is the performance of the Services under the Agreement.

Purpose(s) of the data transfer and further processing

Processing of Personal Data by WTG as necessary to perform the Services under the Agreement.

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

Subject to section 18 of the DPA, WTG will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

For transfers to (Sub-)Processors, also specify subject matter, nature and duration of the Processing

As per section 13 of the DPA, the Subprocessor(s) will Process Personal Data as necessary to perform the Services under the Agreement. Subject to section 18 of the DPA, the Subprocessor(s) will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

A current list of Subprocessors engaged in Processing Personal Data for the performance of each applicable Service – which may be updated by WTG from time to time – can be found on the Privacy Documentation website.

3 COMPETENT SUPERVISORY AUTHORITY

The supervisory authority referred to in section 12.3 of Schedule 2 (EEA/Swiss/UK Specific Transfer Provisions) is the Hamburg Commissioner for Data Protection and Freedom of Information.

Schedule 2 - EEA/Swiss/UK

1 APPLICATION

This Schedule 2 and the EU SCCs as implemented by this Schedule 2 apply if:

(a) either of Controller or its Authorised Affiliates are subject to the Data Protection Laws of the EEA and its member states, Switzerland or the UK; and

(b) Personal Data of Controller or its Authorised Affiliates is being transferred to WTG outside of the EEA, Switzerland or the UK.

2 DATA EXPORTER / DATA IMPORTER

In the EU SCCs, the ICO UK Addendum and this Schedule 2, Controller and Authorised Affiliates are individually or collectively the 'Data Exporter' and WTG is the 'Data Importer'.

3 DOCKING

For clause 7 of the EU SCCs (Docking clause), this option does not apply.

4 SCOPE OF CONTROLLER INSTRUCTIONS

For clauses 8.1(a) and 8.8 of the EU SCCs, the instructions from Controller to Process Personal Data are in section 5 of this DPA and include onward transfers to third parties, including Subprocessors, located outside of the EEA, Switzerland or the UK for the purpose of the performance of the Services.

5 DATA DELETION

For clauses 8.5 and 16(d) of the EU SCCs, the Parties agree that the certification of deletion of Personal Data must be provided by WTG to Controller only upon written request.

6 TOMS

For clause 8.6(a) of the EU SCCs, Controller is solely responsible for making an independent determination as to whether the technical and organisational measures in Annex II to the SCCs meet its requirements. Controller agrees that at the time of execution of the DPA, having taken into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of Personal Data as well as the risks to individuals, the technical and organisational measures taken by WTG provide a level of security appropriate to the risk with respect to the Personal Data.

7 PERSONAL DATA BREACHES

For clause 8.6(c) of the EU SCCs, Personal Data Breaches must be handled in accordance with section 12 of this DPA.

8 INFORMATION REQUESTS AND AUDITS

For clause 8.9 of the EU SCCs, WTG must handle Controller's requests for information and audit requests in accordance with section 10 of this DPA.

9 SUBPROCESSORS

For clause 9(a) of the EU SCCs, the following apply:

(a) WTG has the Controller's general authorisation to engage Subprocessors in accordance with section 13 of this DPA. A current list of Subprocessors engaged in Processing Personal Data for the performance of each applicable Service – which may be updated by WTG from time to time – can be found on the Privacy Documentation website. WTG

must inform the Data Exporter of any changes to Subprocessors following the procedure in section 13 of this DPA.

(b) If WTG enters into EU SCCs (Module 3: Transfer Processor to Processor) with a Subprocessor in connection with the provision of the Services, then Controller hereby grants WTG and its Affiliates authority to provide a general authorisation on behalf of Controller for the engagement of further Subprocessors by Subprocessors engaged in the provision of the Services, as well as decision-making and approval authority for the addition or replacement of any Subprocessors.

10 DATA SUBJECT RIGHTS

For clause 11 of the EU SCCs, and subject to section 8 of this DPA, WTG must inform Data Subjects on its website of a contact point authorised to handle complaints. WTG must inform Controller if it receives a complaint by, or a dispute from, a Data Subject with respect to Personal Data in connection with the provision of the Services and must without undue delay communicate the complaint or dispute to Controller. WTG does not have any further obligation to handle the request, unless otherwise agreed with Controller in each individual case. The option under Clause 11(a) of the EU SCCs does not apply.

11 LIABILITY

For clause 12 of the EU SCCs, the following applies:

(a) WTG's liability under clause 12(a) of the EU SCCs is subject to the limitations of the Agreement;

(b) WTG's liability under clause 12(b) of the EU SCCs is limited to damages caused by its Processing where it has not complied with its obligations under the GDPR specifically directed to Processors, or where it has acted outside of or contrary to lawful instructions of Controller, as specified in Article 82(2) GDPR; and

(c) WTG is exempt from liability under section 11(b) of this Schedule, if it proves that it is not in any way responsible for the event giving rise to the damage under Article 82(3) GDPR.

12 SUPERVISORY AUTHORITY

For clause 13 of the EU SCCs, the following applies:

(a) if Controller is established in an EU member state, then the supervisory authority with responsibility for ensuring compliance by Controller with the GDPR as regards the data transfer is the competent data protection supervisory authority.

(b) if Controller is not established in an EU member state but falls within the territorial scope of application of the GDPR in accordance with its Art. 3(2) and has appointed a representative under Art. 27(1) GDPR, then the supervisory authority of the EU member state, in which the representative within the meaning of Art. 27(1) GDPR is established is the competent data protection supervisory authority.

(c) If the Data Exporter is not established in an EU member state but falls within the territorial scope of application of the GDPR in accordance with its Art. 3(2) without, however, having to appoint a representative under Art. 27(2) GDPR, then the Hamburg Commissioner for Data Protection and Freedom of Information is the competent data protection supervisory authority.

13 REQUESTS FROM AUTHORITIES

For clause 15(1)(a) of the EU SCCs, the following applies:

(a) WTG must notify Controller (only) and not the Data Subject(s) each time it either:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of Personal Data transferred under the EU SCCs; or

(ii) becomes aware of any direct access by public authorities to Personal Data transferred under the EU SCCs in accordance with the laws of the country of destination.

(b) Controller shall be solely responsible for promptly notifying the Data Subject(s) as necessary.

14 GOVERNING LAW

For clause 17 of the EU SCCs, the governing law is the law that applies to the Agreement. If the Agreement is not governed by an EU member state law, the EU SCCs will be governed by the laws of Germany.

15 COURTS

For clause 18(b) of the EU SCCs, the courts will be those designated by the Agreement. If the Agreement does not designate an EU Member State court as having exclusive or non-exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with the Agreement, the Parties agree that the courts of Germany have exclusive jurisdiction to resolve any dispute arising from the EU SCCs.

16 APPENDICES

Appendices to the EU SCCs are completed as follows:

(a) Section A of Schedule 1 to this DPA completes Annex I.A to the EU SCCs.

(b) Section B of Schedule 1 to this DPA completes Annex I.B to the EU SCCs.

(c) Section C of Schedule 1 to this DPA completes Annex I.C to the EU SCCs.

(d) The technical and organisational measures in the description of the TOMs for the relevant Service are Annex II to the EU SCCs.

(e) The current list of Subprocessors engaged in Processing Personal Data for the performance of each applicable Service, which may be updated by WTG from time to time, and which can be found on the Privacy Documentation website, form Annex III to the EU SCCs.

17 TRANSFERS GOVERNED BY THE LAWS OF SWITZERLAND

For transfers of Personal Data governed by the Data Protection Laws of Switzerland, the Parties agree that the EU SCCs will apply in accordance with sections 1 to 16 of this Schedule 2, as further specified below:

(a) general and specific references in the EU SCCs to the GDPR, EU or EU member state law have the same meaning as the equivalent reference in the Data Protection Laws of Switzerland;

(b) for clause 13 of the EU SCCs, the Swiss Federal Data Protection and Information Commissioner is the competent data protection supervisory authority;

(c) for clause 18(b) of the EU SCCs, the courts of Switzerland have exclusive jurisdiction to resolve any dispute arising from the EU SCCs as specified in this section; and

(d) for clause 18(c) of the EU SCCs, the term 'Member State' is not to be interpreted to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland).

18 TRANSFERS GOVERNED BY THE LAWS OF THE UK

For transfers of Personal Data governed by the UK GDPR, the Parties agree to the ICO UK Addendum and its alternative part 2 mandatory clauses, which form an integral part of this DPA. The Parties agree that the EU SCCs apply to these transfers in accordance with sections 1 to 16 of this Schedule 2, and as amended by the mandatory clauses of the ICO UK Addendum. For

section 17 of the ICO UK Addendum, the Parties agree to provide the information of part 1 of the ICO UK Addendum in the following format and as further specified below:

(a) the 'Start Date' for the purposes of part 1 of the ICO UK Addendum is the effective date of the EU SCCs, as specified in section 1.1 of this DPA;

(b) the 'Parties' for the purposes of part 1 of the ICO UK Addendum are WTG as the Data Importer and Controller and its Authorised Affiliates as the Data Exporter(s) as further specified in sections 1 and 2 of this Schedule 2 and section A of Schedule 1;

(c) the 'Key Contacts' for the purposes of part 1 of the ICO UK Addendum are the persons specified in section A of Schedule 1;

(d) the 'Addendum SCCs' for the purposes of part 1 of the ICO UK Addendum are the EU SCCs as specified in sections 1 to 16 of this Schedule 2;

(e) the 'Appendix Information' for the purposes of part 1 of the ICO UK Addendum is the information specified in section 16 of this Schedule 2; and

(f) for part 1 of the ICO UK Addendum, the Data Importer may end the ICO UK Addendum under the conditions in section 19 of the ICO UK Addendum.

Schedule 3 - U.S.

The terms in this Schedule 3 apply to WTG's Processing of Personal Data of U.S. Data Subjects under U.S. Data Protection Laws.

1 DEFINITIONS

In this Schedule 3:

Sell or **Share** has the meaning given in the applicable U.S. Data Protection Law.

U.S. Data Protection Laws means (a) the California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 to 1798.199), as modified by the California Privacy Rights Act, the CCPA Regulations (Cal. Code Regs. tit. 11, §§ 999.300 to 999.337) and any implementing regulations or guidance provided by the California Attorney General or California Privacy Protection Agency, as each of these titles may be amended from time to time ('CCPA'), (b) Virginia Consumer Data Protection Act (Va. Code Ann. §§ 59.1-575-59.1-585), (c) Colorado Privacy Act (Colo. Rev. Stat. §§ 6-1-1301 - 6-1-1313), (d) Connecticut Data Privacy Act (Public Act No. 22-15 §§ 1 - 12), (e) Utah Consumer Privacy Act (Utah Code §§ 13-61-101 to 13-61-404) and (f) other U.S. laws, regulations or requirements or regulatory guidance imposing Sell or Share restrictions on a processor of Personal Data, in each case to the extent applicable to a Party, and any amendments for the forgoing.

2 PROCESSING RESTRICTIONS

2.1 WTG must not:

(a) Sell or Share Personal Data provided to it by Controller for Processing under the Agreement;

(b) retain, use, or disclose Personal Data collected under the Agreement for any purpose other than for the business purposes in the Agreement and this DPA, including but not limited to customs authorities, external service providers and sub processors or as otherwise permitted under applicable U.S. Data Protection Laws;

(c) retain, use, or disclose Personal Data collected under the Agreement for any purpose other than for the commercial purposes set out in the Agreement including but not limited to the provision of the Services and any and all reasonable activities for the purpose of improving or enhancing the Services and this DPA, or as otherwise permitted under applicable U.S. Data Protection Laws; or

(d) retain, use, or disclose Personal Data collected under the Agreement outside the direct business relationship between WTG and Controller, including by combining or updating Controller's Personal Data collected under the Agreement with Personal Data that it received from other sources or collected from its own interaction with a Data Subject except as permitted under applicable U.S. Data Protection Laws.

2.2 For the avoidance of doubt, WTG may collect Personal Data that includes contact information from Controller in connection with the Agreement and the provision of the Services. Controller agrees that in such capacity, WTG is the controller of such information, and further consents to WTG's use of such information to send marketing, advertising, and promotional communications to Controller concerning WTG's and its business partners' products and services that WTG believes may be of interest to Controller.

3 COMPLIANCE AND NOTICE OBLIGATIONS

3.1 WTG will provide the same level of privacy protection of Personal Data provided to it by Controller as required of Controller under applicable U.S. Data Protection Laws.

The Parties agree to comply with applicable U.S. Data Protection Laws. WTG will notify Controller if it makes a determination that it can no longer meet its obligations under applicable U.S. Data Protection Laws, in which case Controller may take reasonable and appropriate steps to stop and remediate any unauthorised use of Personal Data

Schedule 4 - PRC

To the extent WTG (i) Processes Personal Data of Data Subjects in the PRC on behalf of the Customer as Controller and/or (ii) the Controller transfers Personal Data or Other Data out of the PRC to WTG, this Schedule 4 (PRC Specific Transfer and Processing Provisions) shall apply.

1.1 '**Controller**' means the 'personal information handler 'as defined in PIPL or the 'data handler' as defined in other applicable Data Protection Laws.

1.2 '**Other Data**' means important data, core national data and other data subject to export restrictions as defined and set out under PRC Data Protection Laws.

1.3 '**Personal Data**' means 'personal information' as defined in PIPL.

1.4 '**PIPL**' means the PRC Personal Information Protection Law, including any regulations, notices, or other interpretative instruments promulgated or made thereunder.

1.5 '**PRC Data Protection Laws**' include the PRC Cybersecurity Law, the PRC Data Security Law, the PIPL, the Measures on the Standard Contract for the Cross-Border Transfer of Personal Information, the Provisions for the Promotion and Standardization of Cross-Border Data Flows and any other applicable Data Protection Laws issued by the government or any regulatory authority of the PRC, as issued or amended from time to time.

1.6 '**Processing**' or '**Process**' means the collection, storage, use, processing, transmission, provision, disclosure, and deletion of Personal Data.

1.7 '**Processor**' means 'entrusted party' as defined under the PIPL being the party who Processes Personal Data on behalf of and for the purpose of the Controller.

1.8 '**Standard Contract**' means the standard contract under the Measures on the Standard Contract for the Cross-Border Transfer of Personal Information.

1.9 '**Supervisory Authority**' means the Cyberspace Administration of China or any other regulatory authority of the PRC with authority to regulate the collection, transfer and processing of Personal Data and Other Data.

2.1 The Controller and WTG agree to comply with all the provisions and obligations as set out in the Addendum, as read with the relevant provisions of PRC Data Protection Laws in respect of the collection, transfer and Processing of Personal Data or Other Data, as may be applicable.

2.2 The Controller is responsible for providing all required notices and obtaining all required consents from the Data Subjects for transfer of Personal Data to WTG and, if applicable, Authorised Affiliates in or outside of the PRC and represents and warrants that, to the extent required, such notices and consents have been given and obtained in compliance with the requirements of PIPL and other PRC Data Protection Laws.

2.3 If the Controller is restricted from transferring Personal Information out of China under PIPL or any other PRC Data Protection Laws, WTG may immediately discontinue using the relevant portion(s) of the licence, product or service and may terminate the relevant portion(s) of the licence, product or service and WTG shall return or destroy the Personal Data held by it at the choice of the Controller without undue delay.

2.4 WTG agrees to assist the Controller as reasonably required for the Controller to comply with PIPL and other PRC Data Protection Laws, including (i) reporting to a Supervisory Authority or notifying the relevant Data Subjects about a Personal Data breach, (ii) responding to Data Subjects' requests for the exercise of their rights under PIPL, and (iii) providing information to the Controller or its engaged consultants or professional service providers for conducting Personal Data impact assessments or security assessments, as applicable.

2.5 To the extent required by PRC Data Protection Laws, the Controller and WTG agree to enter into stand-alone contractual agreements for the cross-border transfer of Personal Data and Other Data from the Controller to WTG as foreign recipient if the requisite thresholds under the PIPL are met and the Customer informs WTG that the obligation has been met. The parties otherwise

agree that the stand-alone contract shall only be required if Supervisory Authority registration or approval is required.

2.6 The Controller shall notify WTG if it is required to enter into and register a Standard Contract with the Supervisory Authority or obtain approval for the export of Personal Data or Other Data under PRC Data Protection Laws and the legal basis for such requirement.

2.7 The Controller represents and warrants that it shall not transfer any Other Data to WTG without the separate express written consent of WTG.

2.8 The Controller shall indemnify WTG as well as any other applicable WTG Affiliate from any costs, charges, damages, expenses or losses any of them has incurred or any fines that have been imposed on any of them as a result of the Controller violating any of the obligations in the foregoing sections. The Parties agree that the limitations of liability set forth in any other agreement between the parties shall not apply to the indemnification claim under this section.

2.9 WTG shall only disclose the Personal Data to a third party if the third party is or agrees to be bound by this Schedule and the DPA and enters into any required data protection agreement under PRC Data Protection Laws.

3.1 This Schedule and the DPA shall be read and interpreted in light of the provisions of PIPL and other PRC Data Protection Laws. In the event of a conflict between the DPA and this Schedule, this Schedule shall prevail. In the event of a conflict between the Standard Contract or any other agreement for the transfer and Processing of Personal Data or Other Data, that the Controller and WTG separately agree and the DPA, the separate agreement shall prevail.

3.2 This Schedule read together with the DPA shall be governed by and construed in accordance with the laws of the PRC.

3.3 Any dispute arising from this Schedule read together with the DPA shall be resolved by Arbitration in accordance with the Australian Centre for International Commercial Arbitration (ACICA) Arbitration Rules. The seat of arbitration shall be Sydney, Australia. The language of the arbitration shall be English.

Schedule 5 - Taiwan

1 APPLICATION

The Personal Data Protection Act (**PDPA**) applies as specified in this Schedule, which contains operative provisions for the implementation of the PDPA, to Controller and its Authorised Affiliates if either of these entities are subject to the PDPA and any of their Personal Data is transferred to WTG or its Affiliates outside of Taiwan.

2 DATA EXPORTER / DATA IMPORTER

For the PDPA and this Schedule 5, the Controller and Authorised Affiliates are individually or collectively the 'Data Exporter' and WTG is the 'Data Importer'.

3 DEFINITIONS

In this Schedule 5:

Personal Data has the meaning given in the PDPA and refers to a natural person's name, date of birth, national identification card number, passport number, physical characteristics, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, sex life, records of physical examination, criminal records, contact information, financial conditions, social activities and any other information that may be used to directly or indirectly identify a natural person. 'Personal Data' includes 'special categories of personal data' or 'sensitive personal data'.

Non-Government Agency has the meaning given in the PDPA and refers to a natural person, legal person or group other than a government agency. In complying with the obligations in the DPA, 'Non-Government Agency' replaces and substitutes 'Controller' in the DPA.

Commissioned Agency refers to a person or entity that Processes Personal Data under the commission or on behalf of others. In complying with the obligations in the DPA, 'Commissioned Agency' replaces and substitutes the term 'Processor' in the DPA.

Processing or **Process** means any operation or set of operations performed on the Personal Data, which falls within the meaning of 'processing' or 'use' as defined in the PDPA, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

PDPA, means the Personal Data Protection Act, which includes the Enforcement Rules of the PDPA (the **Enforcement Rules**) and other laws, regulations and rules relating to the protection of Personal Data in Taiwan.

Proper Security Measures means the technical or organisational measures taken by Non-Government Agency for the purpose of preventing Personal Data from being stolen, altered, damaged, destroyed or disclosed, in accordance with Article 12 of the Enforcement Rules.

4 INTERNATIONAL TRANSFER OF PERSONAL DATA

4.1 The Parties agree that the Non-Government Agency may transfer Personal Data to WTG, and WTG may receive and Process that Personal Data, subject to this Schedule 5 and this DPA.

4.2 For Article 21 of the PDPA, Non-Government Agency must not transfer any Personal Data to WTG if the Taiwan central government authority in charge of the industry concerned has imposed restrictions on the transfer under any of the following circumstances:

(a) where major national interests of Taiwan are involved;

(b) where an international treaty or agreement so stipulates;

(c) where the country receiving the Personal Data lacks proper regulations on protection of Personal Data and the Data Subject's rights and interests may consequently be harmed; or

(d) where the cross-border transfer of the Personal Data to a third country (territory) is carried out to circumvent the PDPA.

5 OBLIGATIONS OF THE DATA EXPORTER AND DATA IMPORTER

5.1 For Article 13 of the PDPA and subject to section 8 of this DPA, WTG must promptly notify Non-Government Agency of any request made by a Data Subject to WTG under Article 10 of the PDPA and shall without undue delay communicate the request to Non-Government Agency. Non-Government Agency must determine whether to accept or reject the request within 15 days; the deadline may be extended by up to 15 days if necessary, and Non-Government Agency must notify the Data Subject in writing of the reason for the extension.

5.2 For Article 13 of the PDPA, WTG must promptly notify Non-Government Agency of any request or dispute made by a Data Subject to WTG under Article 11 of PDPA and shall without undue delay communicate the request to Non-Government Agency. Non-Government Agency must determine whether to accept or reject the request within 30 days; the deadline may be extended by up to 30 days if necessary, and Non-Government Agency must notify the Data Subject in writing of the reason for the extension.

5.3 For Article 27 of the PDPA, Non-Government Agencies in possession of Personal Data must implement Proper Security Measures to prevent the Personal Data from being stolen, altered, damaged, destroyed or disclosed. Taiwan central government authorities in charge of the industries concerned may designate and order certain Non-Government Agency to establish a security and maintenance plan for the protection of Personal Data and rules of disposing Personal Data following a business termination. Non-Government Agency shall comply with the plans and disposal regulations established by the central government authority in charge of the industry concerned.

6 GOVERNING LAW AND JURISDICTION

6.1 For Article 51 of the PDPA, this Schedule 5 read together with the DPA is governed by the laws of the Republic of China (Taiwan).

6.2 The Parties agree that the Taiwan Taipei District Court has exclusive jurisdiction to resolve any dispute, controversy or claim arising out of or related to this Schedule 5.

Schedule 6 - Australia

This Schedule 6 applies to the transfer of Personal Data of individuals in Australia by Controller to WTG outside Australia, for the Services provided under the Agreement (**Australian Transfers**).

1 DEFINITIONS

1.1 In this Schedule:

APPs means the Australian Privacy Principles set out in Schedule 1 of the Privacy Act.

Privacy Act means the *Privacy Act 1998* (Cth) and includes any successor or replacement legislation.

2 APPS GENERALLY

2.1 The DPA addresses the requirements of the APPs in relation to Australian Transfers.

3 CROSS-BORDER DISCLOSURES

3.1 For the purposes of APP 8 (Cross-border disclosure of personal information), the DPA describes:

(a) applicable laws to which WTG is subject to protect information disclosed to WTG by Controller; and

(b) steps that WTG takes to protect information.

Schedule 7 - Brazil

This Schedule 7 applies to the transfer of Personal Data of individuals in Brazil (**Brazil Personal Data**) by Controller to WTG outside Brazil, for the Services provided under the Agreement (**Brazilian Transfers**).

1 PROCESSING PROVISIONS

1.1 For section 6 of this DPA, WTG is considered a controller, when it Processes Personal Data for its own purposes of Product Development.

1.2 For section 12 of this DPA, if WTG is a controller under clause 1.1 of this Schedule 7 for Personal Data affected by a Personal Data Breach, then in addition to notifying Controller WTG must notify the Brazilian Data Protection Authority (**ANPD**) within 3 business days upon learning of the Personal Data Breach.

2 TRANSFER PROVISIONS

2.1 For this Schedule:

(a) Controller is the 'Data Exporter';

(b) WTG is the 'Data Importer'; and

(c) Data Exporter and Data Importer are jointly referred to as 'Parties'.

2.2 Schedule 2 (EEA/Swiss/UK) of this DPA applies to Brazilian Transfers with the following changes:

(a) any reference to 'Data Protection Laws of the EEA and its member states, Switzerland or the UK, including but not limited to the GDPR' shall mean data protection laws, directives or regulations applicable in Brazil, including, but not limited to the Law No. 13,709/2018 (Brazilian Data Protection Law or 'LGPD');

(b) references to 'EU Member State' or 'Member State' refer to the territory of Brazil;

(c) references to court jurisdiction and supervisory authority refer to the courts and supervisory authority of Brazil. Any dispute between the Parties in connection with the international transfer of Brazil Personal Data are to be resolved before the relevant courts of Brazil. All complaints by Data Subjects in connection with the international transfer of Brazil Personal Data are subject to the jurisdiction of the ANPD, as applicable; and

(d) general and specific references in the EU SCCs to the GDPR, EU or EU member state law have the same meaning as the equivalent reference in the LGPD.

Schedule 8 - Turkey

1 TRANSFER PROVISIONS

1.1 Under Turkish Data Protection Law No. 6698 (**Turkish DP Law**), the Turkish Standard Contracts as announced by the Turkish Personal Data Protection Authority (**Turkish Authority**) on its website (**Turkish SCs**) must be executed between Controller (on its own behalf and on behalf of its Authorised Affiliates) and WTG for the transfer of Personal Data to third countries other than Turkey and the executed Turkish SCs shall be an integral part of this DPA.

1.2 The Turkish SCs apply as further specified in this Schedule, which contains operative provisions for the implementation of the Turkish SCs to Controller and its Authorised Affiliates, if either of Controller or its Authorised Affiliates is subject to the Turkish DP Law and Personal Data of these entities is being transferred to WTG outside of Turkey and in this case, the Parties agree to execute Turkish SCs and submit it to the Turkish Authority within five business days following its execution. The Parties must also notify the Turkish Authority within five business days in case of a change in the parties or the content of the Turkish SCs or the termination of the Turkish SCs.

1.3 For the Turkish SCs and this Schedule 8, Controller and its Authorised Affiliates are individually or collectively the 'Data Exporter' and WTG is the 'Data Importer'.

1.4 For Clauses 7.1(a) and 7.8 of the Turkish SCs, the instructions from Controller or its Authorised Affiliates to Process Personal Data and onward transfers to third parties are subject to section 5 of this DPA, including Subprocessors, located outside of Turkey for the purpose of the performance of the Services.

1.5 For Clauses 7.4 and 15(d) of the Turkish SCs, the Parties agree that the certification of deletion of Personal Data shall be provided by WTG to Controller only upon written request.

1.6 For Clause 7.6(a) of the Turkish SCs, Controller is solely responsible for making an independent determination as to whether the technical and organisational measures in Annex II to the Turkish SCs meet its requirements. Controller agrees that at the time of execution of the DPA, having taken into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the Processing of Personal Data as well as the risks to individuals, the technical and organisational measures taken by WTG provide a level of security appropriate to the risk with respect to the Personal Data.

1.7 For Clause 7.6(c) of the Turkish SCs, Personal Data Breaches must be handled in accordance with section 12 of this DPA provided that the Parties shall follow the procedures for each Personal Data Breach set out in the decisions of the Turkish Personal Data Protection Board ('Turkish Board') dated 24.01.2019 numbered 2019/10 and dated 18.09.2019 numbered 2019/271.

1.8 For Clause 7.8. of the Turkey SCs, WTG must handle Controller's requests for information and audit requests in accordance with section 10 of this DPA to the extent that the conditions in Clause 7.9. of the Turkish SCs are met.

1.9 For Clause 8(a) of the Turkish SCs, the following applies:

(a) WTG has Controller's general authorisation to engage Subprocessors in accordance with section 13 of this DPA. A current list of Subprocessors engaged in Processing Personal Data for the performance of each applicable Service – which may be updated by WTG from time to time – can be found on the Privacy Documentation website. WTG must inform the Data Exporter of any changes to Subprocessors following the procedure in section 13 of this DPA.

(b) If WTG enters into respective Turkish SCs which regulate 'Transfer Processor to Processor' with a Subprocessor in connection with the provision of the Services, then Controller grants WTG and its Affiliates authority to provide a general authorisation on behalf of Controller for the engagement of further Subprocessors by Subprocessors engaged in the provision of the Services, as well as decision-making and approval authority for the addition or replacement of any Subprocessors.

1.10 For Clause 10 of the Turkish SCs, and subject to section 8 of this DPA, WTG must inform Data Subjects on its website of a contact point authorised to handle complaints. WTG must inform Controller if it receives a complaint by, or a dispute from, a Data Subject with respect to Personal Data in connection with the provision of the Services and must without undue delay communicate the complaint or dispute to Controller. Except for the obligations in Clause 10 of the Turkish SCs, WTG has no further obligation to handle the request, unless otherwise agreed with Controller in each individual case. The option under Clause 10(a) of the Turkish SCs shall not apply.

1.11 For Clause 11 of the Turkish SCs, the following applies:

(a) WTG's liability under Clause 11(a) of the Turkish SCs shall be subject to the limitations of the Agreement.

(b) WTG's liability under Clause 11(b) of the Turkish SCs shall be limited to any damage caused by its Processing where it has acted outside of or contrary to lawful instructions of Controller.

(c) WTG shall be exempt from liability under section 11(b) of this Schedule 8, if it proves that it is not in any way responsible for the event giving rise to the damage.

1.12 For Clause 12 of the Turkish SCs, the following applies:

(a) the supervisory authority with responsibility for ensuring compliance by Controller with the Turkish DP Law and its secondary legislation shall be the Turkish Authority; and

(b) if Controller is not established in Turkey but falls within the territorial scope of application of the Turkish DP Law and has appointed a representative under Art. 11 of the Regulation on the Data Controllers' Registry, then the supervisory authority shall be the Turkish Authority and shall act as competent data protection supervisory authority.

1.13 For Clause 14 of the Turkish SCs, the following applies:

(a) WTG must notify Controller (only) and not the Data Subject(s) in each and every case it receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of Personal Data transferred under the Turkish SCs; and

(b) Controller shall be solely responsible for promptly notifying the Data Subject(s) as necessary.

1.14 For Clause 17 of the Turkish SCs, the governing law is Turkish Law.

1.15 Any dispute arising out of this Schedule8 and Turkish SCs is governed by Turkish laws and the Parties agree to acknowledge the exclusive judicial authority of İstanbul Çağlayan courts.

1.16 The Appendix to the Turkish SCs shall be completed as follows:

(a) Annex I of the Turkish SCs shall be filled-out in line with section A and section B of Schedule 1 (Description of Processing) of this DPA. In addition to the information indicated in Schedule 1 (Description of Processing) of this DPA, the Data Controllers' Registry System information of the Data Exporter shall be indicated;

(b) the technical and organisational measures in the description of the TOMs for the relevant Service are Annex II to the Turkish SCs; and

(c) the current list of Subprocessors engaged in Processing Personal Data for the performance of each applicable Service, which may be updated by WTG from time to time, and which can be found on the Privacy Documentation website, is Annex III to the Turkish SCs.

2 PROCESSING PROVISIONS

2.1 The Parties agree to process and transfer Special Categories of Personal Data by taking the measures specified in the decision of the Turkish Board dated 31.01.2018 and numbered 2018/10 on 'Adequate Measures to be Taken by Data Controller for the Processing of Special Categories

of Personal Data', if the Processor Processes the Special Categories of Personal Data on behalf of Controller.

2.2 If it is a Processor, then WTG accepts and undertakes that it shall be subject to a duty of confidentiality with respect to the Personal Data that it Processes on behalf of Controller for an indefinite period.

2.3 If both Parties are deemed as a Controller, then Controller agrees, declares and undertakes that;

(a) the Personal Data transferred to WTG has been collected, Processed, and transferred to WTG in compliance with the Turkish DP Law and its secondary legislation; and

(b) in case of a Personal Data Breach or an incident that might be qualified as a Personal Data Breach, Clause 1.7 of section 1 of this Schedule also applies to Controller.

2.4 If a Party receives an application from a Data Subject or a request/notification from public institutions or organisations with regard to Personal Data Processing which is essentially under the responsibility of the other Party, then the receiving Party shall provide the other Party with the relevant application, request or notification and the Parties must provide each other with the necessary information or documents in order to enable the responsible Party to respond to the relevant application, request or notification in a timely manner.

2.5 The Parties agree that the Parties' Processors will comply with the undertakings given to the other Party under this Schedule and that Controller is directly liable to the other Party for any damages that may arise from non-compliance by its Processors with these undertakings.

Controller accepts, declares, and undertakes to appropriately inform Data Subjects on behalf of WTG by providing the privacy notice of WTG, which can be found on the WiseTech Global website , regarding (i) the Processing of Controller's Personal Data if Controller is a natural person, and (ii) the Processing of the Personal Data of Controller's employees or officials.