

## **Data Protection Schedule**

*If you process personal data on behalf of the Tag, the following terms shall apply. These terms are supplementary to the Main Terms and Conditions ("the Main Terms"). All capitalised terms that are not defined in this Appendix shall have the definitions set out in the Main Terms. The particulars of processing under this schedule below and its annexes should be completed as appropriate to the processing.*

### **1. INTRODUCTION**

- 1.1 Pursuant to an agreement dated [*insert date*] (the "**Services Agreement**"), the Supplier shall provide certain services (the "**Services**") to the Agency. To the extent that the Supplier is processing Agency Personal Data as part of the Services, the terms contained in this Data Processing Agreement (the "**Agreement**") will apply.
- 1.2 If the Services are altered during the term of the Agreement and the altered Services involve new or amended processing of Personal Data, the parties will ensure that Annex 1 is updated as appropriate before such processing commences.
- 1.3 If the Data Protection Legislation is amended during the term of the Agreement in a way that affects the compliance of this Schedule with the Data Protection Legislation, the parties will ensure that this Schedule is updated as appropriate as soon as reasonably practicable.

### **2. DEFINITIONS**

- 2.1 For the purposes of this schedule (the "**Schedule**"), capitalised terms have the meanings given below:

**"Agreement"** means the contract between the Tag and the Supplier to which this Schedule is attached, pursuant to which the Supplier provides Services to the Tag.

**"Applicable Law"** means (i) any and all laws, statutes, regulations, by-laws, orders, ordinances and court decrees that apply to the performance and supply of the Services or the processing of Personal Data under the Agreement, and (ii) the terms and conditions of any applicable approvals, consents, exemptions, filings, licences, authorities, permits, registrations or waivers issued or granted by, or any binding requirement, instruction, direction or order of, any applicable government department, authority or Tag having jurisdiction in respect of that matter.

**"Client"** means any client(s) of the Tag from time to time for whom the Services are for the ultimate benefit.

**"Data Protection Legislation"** means all Applicable Laws and codes of practice applicable to the processing of personal data including, where applicable, the GDPR,.

**"GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data as applicable as of 25 May 2018, as may be amended from time to time.

**"Losses"** means all liabilities, including all:

- (a) costs (including legal costs), claims, demands, actions, settlements, ex-gratia payments, charges, procedures, expenses, losses and damages (including relating to material and non-material damage); and
- (b) to the extent permitted by Applicable Law:
  - (i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a court or regulatory authority;
  - (ii) compensation to a data subject ordered by a court or regulatory authority; and
  - (iii) the costs of compliance with investigations by a regulatory authority.

**“Non-Adequate Recipient”** means a recipient of Personal Data which is established in a country or territory which has not been recognised by a relevant competent supervisory authority or another competent authority (including the European Commission) as providing an adequate level of protection to personal data.

**“Personal Data”** means personal data provided or made available to the Supplier by or on behalf of a Client, or collected or created by the Supplier in the course of delivering the Services and includes but is not limited to the personal data set out in Annex 1 and which is processed by the Supplier for and on behalf of the Client in the performance of the Services.

**“Personal Data Breach”** means an actual or suspected breach of security leading to the accidental, unauthorised or unlawful destruction loss, alteration disclosure of, or access to, Personal Data while in the custody of the Supplier or a Sub-Processor.

**“Restricted Transfer”** means a transfer of Personal Data to a Non-Adequate Recipient which may be rendered permissible under Data Protection Legislation where a Transfer Mechanism is validly used in order to make and govern the transfer.

**“Services”** means the services to be provided by the Supplier pursuant to the Agreement, as further explained in clause 1.1 of this Schedule.

**“Standard Contractual Clauses”** or **“SCCs”** means a set of contractual provisions approved or otherwise recognised by a relevant competent supervisory authority as enabling an international transfer or personal data to be made in compliance with Data Protection Legislation including, (i) in the EEA, the contractual provisions found in decision 2021/914 of the European Commission (**“EEA SCCs”**) (ii) for ASEAN, the ASEAN Model Contractual Clauses for Cross Border Data Flows (**“ASEAN MCCs”**), (iii) for Hong Kong, the Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data (**“HK RMCs”**), (iv) for New Zealand, the Model Contract Clauses Agreement (**“NZ Model Agreement”**), and (v) for China, the Standard Contract for Outbound Transfer of Personal Information (**“China Standard Contract”**) issued by the Cyberspace Administration of China.

**“Sub-Processor”** means any further sub-processor engaged by the Supplier for carrying out processing activities in respect of the Personal Data on behalf of the Tag and authorised by the Tag in accordance with clause 6.7 of this Schedule.

**“Supplier”** has the meaning set out in the Agreement.

**“Transfer Mechanism”** means any means of transferring personal data from a data exporter to a data importer, permitted under the Data Protection Legislation, including the Standard Contractual Clauses.

2.2 Where this Schedule uses the terms defined in the Data Protection Legislation, those terms shall have the same meaning as in the Data Protection Legislation.

2.3 This Schedule is to be read and interpreted in the light of the provisions of the Data Protection Legislation and must not be interpreted in a way that runs counter to the rights and obligations provided for in the Data Protection Legislation, or in a way that prejudices the fundamental rights or freedoms of data subjects.

### 3. PURPOSE AND SCOPE

3.1 The purpose of this Schedule is to ensure compliance with the Data Protection Legislation.

3.2 This Schedule applies to the processing of Personal Data as set out in paragraph 5 and as specified in Annex 1.

3.3 This Schedule is without prejudice to obligations to which the Tag and the Supplier are subject by virtue of the Data Protection Legislation.

## **4. HIERARCHY**

### **4.1 In the event of a contradiction or inconsistency between:**

- 4.1.1 this Schedule and the provisions of the Agreement or any other agreement between the parties existing at the time when this Schedule is agreed or entered into thereafter, this Schedule will prevail; or
- 4.1.2 where there is Restricted Transfer, this Schedule and any applicable Transfer Mechanism, then the applicable Transfer Mechanism will prevail; or
- 4.1.3 an applicable Transfer Mechanism and another applicable Transfer Mechanism, the Transfer Mechanism which affords the highest level of protection to the rights and freedoms of the data subjects will prevail,

in each case, solely to the extent of such contradiction or inconsistency.

## **5. DESCRIPTION OF PROCESSING**

The details of the processing operations, their purposes, scope and duration, and the categories of Personal Data permitted to be processed by the Supplier in connection with the Agreement are set out in Annex 1.

## **6. OBLIGATIONS OF THE PARTIES**

### **6.1 Instructions**

- 6.1.1 The Supplier must process Personal Data only on documented instructions from the Tag, unless required to do so by Applicable Law to which the Supplier is subject. In this case, the Supplier must inform the Tag of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Tag throughout the duration of the processing of Personal Data. These instructions must always be documented.
- 6.1.2 The Supplier must immediately inform the Tag if, in the Supplier's opinion, instructions given by the Tag infringe the Data Protection Legislation. Following such notification the Tag will have the right to suspend the relevant processing instructions and either amend them (to the extent the Tag considers this is necessary for the purpose of complying with Data Protection Legislation) or terminate that part of the processing by the Supplier. In the event of such suspension or termination, to the extent that any elements of the fees and/or charges under the Agreement relate to such processing instruction, such fees and/or charges will not be payable by the Tag and the Supplier waives any right it may have to such amounts.
- 6.1.3 The Supplier must contact the Tag as soon as reasonably practicable if it is ever unsure as to the parameters of any processing instructions of the Tag.

### **6.2 Purpose limitation**

The Supplier is permitted to process the Personal Data only for the specific purpose(s) of the processing, as set out in this Schedule and the Agreement including Annex 1, unless it receives further instructions from the Tag.

### **6.3 Duration of the processing of Personal Data**

Processing by the Supplier must only take place for the duration specified in Annex 1.

### **6.4 Security of processing**

6.4.1 The Supplier must, at its own cost and expense, at least implement the technical and organisational measures specified in Annex 3 to ensure the security of the Personal Data, including protecting the Personal Data against a Personal Data Breach. In assessing the appropriate level of security, the parties will 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.

6.4.2 The measures referred to in clause 6.4.1 must at all times:

- (a) be of at least the minimum standard required by Data Protection Legislation;
- (b) be of a standard no less than the standards compliant with good industry practice for the protection of personal data; and
- (c) be compliant with any minimum standards and/or requirements that the Tag may provide to the Supplier from time to time in writing.

6.4.3 The Supplier may grant access to the Personal Data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the Agreement. The Supplier must (and must procure its Sub-Processors must) ensure that persons authorised to process the Personal Data:

- (a) are reliable and have received adequate training on compliance with this Schedule and the Data Protection Legislation;
- (b) do not process Personal Data other than in accordance with processing instructions that the Tag gives in accordance with clause 6.1.1 except where processing of Personal Data is required by Applicable Law in which case the Supplier must, where practicable and not prohibited by Applicable Law, notify the Tag of any such requirement before processing in accordance with clause 6.1.1; and
- (c) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

## **6.5 Sensitive data and critical data**

The parties agree that personal data which: (i) relates to minors (being a data subject under the age of 16 or such other age as defined under Applicable Law); or (ii) reveals the racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences; [(iii) identification number; (iv) bank account number; (v) passwords] ("**sensitive data**") and critical data which may have a serious impact on state security or public interest if such data is leaked ("**critical data**") will not be processed by the Supplier under this Schedule without specific written agreement between the parties. If the parties agree that sensitive data will be processed by the Supplier under the Agreement, then they may agree to and document specific restrictions and additional safeguards prior to the commencement of the processing including the requirement to conduct a data protection impact assessment (clause 7.4.1 below) as may be required under Data Protection Legislation.

## **6.6 Documentation and compliance**

6.6.1 The parties must be able to demonstrate compliance with this Schedule.

6.6.2 The Supplier must deal promptly and adequately with inquiries from the Tag about the processing of Personal Data in accordance with this Schedule.

- 6.6.3 The Supplier must (and must procure that any Sub-Processor must), at no cost to the Tag, make available to the Tag all information necessary to demonstrate compliance with the obligations that are set out in this Schedule or which stem directly from the Data Protection Legislation.
- 6.6.4 At the Tag's request, the Supplier must (and must procure that any Sub-Processor must), at no cost to the Tag, also permit and contribute to audits of the processing activities covered by this Schedule, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Tag may take into account relevant certifications held by the Supplier.
- 6.6.5 The Tag may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Supplier and will, where appropriate, be carried out with reasonable notice.
- 6.6.6 If any audit or inspection reveals non-compliance by the Supplier (or any Sub-Processor) with its obligations under Data Protection Legislation or a breach by the Supplier of its obligations under this Schedule, the Supplier must promptly at the request of the Tag:
- (a) pay the costs of the Tag (or its qualified representative) of the audit or inspection; and
  - (b) resolve (and must procure that any Sub-Processor resolves), at its own cost and expense all data protection and security issues discovered during the audit or inspection which reveal a breach or potential breach by the Supplier (or any Sub-Processor) of its obligations under this Schedule.
- 6.6.7 The parties will make the information referred to in this clause 6.6, including the results of any audits, available to the competent supervisory authority/ies on request.

## **6.7 Use of Sub-Processors**

- 6.7.1 The Supplier may not subcontract any of its processing operations performed on behalf of the Tag in accordance with this Schedule to a Sub-Processor, without the Tag's prior specific written authorisation. The Supplier must submit a request for specific authorisation at least 2 weeks prior to the engagement of the Sub-Processor in question, together with the information necessary to enable the Tag to determine whether or not to grant any authorisation. The list of Sub-Processors authorised by the Tag can be found in Annex 2 or as may be agreed between the parties in writing. The Supplier must maintain a list of authorised Sub-Processors and provide such list to the Tag on request.
- 6.7.2 Where the Supplier engages a Sub-Processor for carrying out specific processing activities (on behalf of the Tag), it must:
- (a) enter a contract which imposes on the Sub-Processor data protection obligations which are not less restrictive than those imposed on the Supplier under this Schedule;
  - (b) ensure that the Sub-Processor complies with the obligations to which the Supplier is subject under this Schedule and the Data Protection Legislation;
  - (c) keep a written record containing at least the following information in relation to each Sub-Processor: (i) all of the information set out in by Annex 2; (ii) the date on which the Tag gave the written approval referred to in clause 6.7.1; and (iii) the name and job title of the person who gave

such written approval on behalf of the Tag. The Supplier must, on request, make a copy of this record available to the Tag; and

- (d) immediately cease using a Sub-Processor to process Personal Data upon receiving written notice from the Tag directing the Supplier to do so.

6.7.3 At the Tag's request, the Supplier must promptly provide a copy of the relevant Sub-Processor agreement that is referred to in clause 6.7.2(a) and any subsequent amendments to the Tag.

6.7.4 The Supplier remains fully responsible to the Tag for the performance of the Sub-Processor's obligations, as well as for any acts or omissions of the Sub-Processor as regards its processing of Personal Data. The Supplier must notify the Tag of any failure by the Sub-Processor to fulfil its contractual obligations.

6.7.5 The Supplier must agree to a third party beneficiary clause with the Sub-Processor whereby - in the event the Supplier has factually disappeared, ceased to exist in law or has become insolvent - the Tag has the right to terminate the Sub-Processor contract and to instruct the Sub-Processor to erase or return the Personal Data.

## **6.8 International transfers**

### ***Transfers between the Tag and Supplier***

6.8.1 To the extent that the provision of the Services by the Supplier requires a Restricted Transfer between the Tag (acting as the 'data exporter') and the Supplier (acting as the 'data importer'), the parties will ensure that an agreed Transfer Mechanism will govern such Restricted Transfer, which may include the Standard Contractual Clauses (as may be relevant between a controller and a processor or a processor and a sub-processor) if the Tag determines that the Standard Contractual Clauses constitute the appropriate Transfer Mechanism in respect of such Restricted Transfer.

6.8.2 Where a Restricted Transfer set out in clause 6.8.1 would result in the transfer of Personal Data from the European Economic Area to a Non-Adequate Recipient outside the European Economic Area, Annex 4 will apply to such Restricted Transfers. Where a Restricted Transfer set out in clause 6.8.1 would result in the transfer of Personal Data from an APAC jurisdiction to a Non-Adequate Recipient outside such APAC jurisdiction, Annex 6 will apply to such Restricted Transfers

6.8.3 The Supplier must implement and maintain technical and organisational measures to ensure that Personal Data is subject to a level of security appropriate to risks arising from its processing and the processing of Sub-Processors.

### ***Onward transfers between the Supplier and third parties***

6.8.4 The Supplier must not (and must procure that Sub-Processors must not) carry out a Restricted Transfer of Personal Data without the prior written approval of the Tag.

6.8.5 Where the Tag provides its consent in accordance with clause 6.8.4 above, the Supplier must ensure that any such transfer of Personal Data:

- (a) takes place in compliance with the Data Protection Legislation; and
- (b) is conducted subject to and in accordance with a Transfer Mechanism agreed with the Tag, as set out in Annex 2 or as otherwise agreed with the Tag in writing.

- 6.8.6 Transfers approved by the Tag as at the date of the Agreement are set out in Annex 2.
- 6.8.7 In respect of any Restricted Transfers to be made between the Supplier and a Sub-Processor, the Supplier must implement and maintain all appropriate technical, organisational and contractual measures to ensure that the Transfer Mechanism used to govern each Restricted Transfer is rendered effective and compliant with the Data Protection Legislation (together, the **"Supplemental Measures"**).
- 6.8.8 The Supplier warrants that it is and will at all times be compliant with: i) the obligations of any Transfer Mechanism; and ii) the Supplemental Measures referred to in clause 6.8.7 of this Schedule.

### ***New Transfer Mechanisms***

- 6.8.9 Where any updates or amendments to, or replacement of, a Transfer Mechanism is approved by the competent authority/ies during the term of the Agreement (**"New Transfer Mechanism"**), the parties will work together to agree and to put in place a New Transfer Mechanism and the Tag shall have no liability under the Agreement as a result of the suspension of a Transfer Mechanism.

## **7. ASSISTANCE TO THE TAG**

- 7.1 The Supplier must (at no cost to the Tag) promptly (and in any event within 3 calendar days of receipt) notify the Tag of any request it receives from a data subject. The Supplier must not respond to the request itself, unless authorised to do so by the Tag, and must provide the Tag with such information, co-operation and assistance as the Tag requires in relation to each such request.
- 7.2 The Supplier must (at no cost to the Tag) promptly (and in any event within 48 hours of receipt) notify the Tag of any complaint that it receives from a data subject or a competent supervisory authority relating to the processing of Personal Data. The Supplier must not respond to the complaint unless authorised to do so by the Tag, and must provide the Tag with such information, co-operation and assistance as the Tag requires in relation to each such complaint.
- 7.3 The Supplier must (at no cost to the Tag) promptly (and in any event within 3 calendar days of receipt) notify the Tag of any enquiry it receives from a third party (which may include any competent supervisory authority) relating to the processing of Personal Data. The Supplier must not respond to the enquiry unless authorised to do so by the Tag, and must provide the Tag with such information, co-operation and assistance as the Tag requires in relation to each such enquiry.
- 7.4 The Supplier must assist the Tag in:
  - 7.4.1 carrying out any assessment of the impact of the envisaged processing operations on the protection of Personal Data (a 'data protection impact assessment') where in the Tag's sole opinion or otherwise at any competent supervisory authority's direction the processing is likely to result in a high risk to the rights and freedoms of natural persons;
  - 7.4.2 any obligation to consult any competent supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Tag to mitigate the risk;

- 7.4.3 ensuring that Personal Data is kept accurate and up to date, by informing the Tag without delay if the Supplier becomes aware that the Personal Data it is processing is inaccurate or has become outdated; and
  - 7.4.4 the Tag's compliance with obligations under Data Protection Legislation in respect of technical and organisational measures to be applied to Personal Data processed by the Supplier.
- 7.5 The Supplier must:
  - 7.5.1 maintain a record of all categories of processing carried out on behalf of the Tag;
  - 7.5.2 make the same available to the Tag and to any relevant regulatory authority (providing a copy of any such correspondence to the Tag) on request; and
  - 7.5.3 comply with all reasonable requests or directions by the Tag to verify and/or procure the Supplier's full compliance with its obligations under Data Protection Legislation and this Schedule.

## **8. NOTIFICATION OF A PERSONAL DATA BREACH**

- 8.1 In the event of a Personal Data Breach, the Supplier must cooperate with and assist the Tag for the Tag to comply with its relevant obligations under the Data Protection Legislation, where applicable, taking into account the nature of processing and the information available to the Supplier.
- 8.2 In the event of a Personal Data Breach, the Supplier must notify the Tag without undue delay and in any event in no later than twelve (12) hours, after the Supplier having become aware of, or receiving a notification regarding, or first suspecting the Personal Data Breach. The Supplier must, without undue delay, and in any event no later than twenty four (24) hours after becoming aware of, or receiving a notification regarding, or first suspecting the Personal Data Breach provide the Tag with detailed information which must contain, at least:
  - 8.2.1 a description of the nature of the Personal Data Breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
  - 8.2.2 the details of a contact point where more information concerning the Personal Data Breach can be obtained; and
  - 8.2.3 its likely consequences and the measures taken or proposed to be taken to address the Personal Data Breach, including to mitigate its possible adverse effects.
- 8.3 Where it is not possible to provide all this information at the same time, the initial notification must contain the information then available and further information must, as it becomes available, subsequently be provided without undue delay.
- 8.4 The Supplier must take all necessary steps to mitigate the effects and to minimise any damage resulting from the personal data breach and to prevent a recurrence of such personal data breach.
- 8.5 The Supplier must assist the Tag's affected Client(s) in notifying the Personal Data Breach to relevant competent supervisory authorities, without undue delay after the Supplier has become aware of the Personal Data Breach.

## **9. NON-COMPLIANCE WITH THIS SCHEDULE AND TERMINATION**

- 9.1 Without prejudice to any provisions of Data Protection Legislation, in the event that the Supplier is in breach of its obligations under this Schedule, the Tag may instruct the Supplier to suspend the processing of Personal Data until the Supplier complies with this Schedule or until the Agreement (or relevant parts thereof) is terminated. The Supplier must promptly inform the Tag if it is unable to comply with this Schedule.
- 9.2 The Tag is entitled to terminate the Agreement insofar as it concerns processing of Personal Data in accordance with this Schedule if:
- 9.2.1 the processing of Personal Data by the Supplier has been suspended by the Tag pursuant to clause 9.1 and if compliance with this Schedule is not restored within a reasonable time and in any event within 1 month following suspension;
  - 9.2.2 the Supplier is in substantial or persistent breach of this Schedule or its obligations under the Data Protection Legislation;
  - 9.2.3 the Supplier fails to comply with a binding decision of a competent court or a competent supervisory authority regarding its obligations under this Schedule or the Data Protection Legislation.
- 9.3 The Supplier is entitled to terminate the Agreement insofar as it concerns processing of Personal Data under this Schedule where, after having informed the Tag that its instructions infringe applicable legal requirements in accordance with clause 6.1.2, the Tag insists on compliance with the instructions.
- 9.4 Following termination of the Schedule for any reason, the Supplier must, at the choice of the Tag, delete all Personal Data processed on behalf of the Tag and certify to the Tag that it has done so, or return all the Personal Data to the Tag and delete existing copies unless Applicable Law requires storage of the Personal Data, in which case the Supplier must demonstrate the Applicable Law relied upon to the satisfaction of the Tag. Until the data is deleted or returned, the Supplier must continue to ensure compliance with this Schedule.

## **10. LIMITATION OF LIABILITY**

- 10.1 The Tag's total aggregate liability to the Supplier in contract, tort (including negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, arising in connection with the performance or contemplated performance of this Schedule or any collateral contract will in all circumstances be limited to 100% of the fees paid to the Supplier in the 12 months preceding the event triggering its liability.
- 10.2 Where both parties are responsible for the act, or omission to act, resulting in the payment of Losses by a party or both parties, then each party shall only be liable for that part of such Losses which is in proportion to its respective responsibility.

## **11. INDEMNITY**

- 11.1 The Supplier shall indemnify and keep indemnified the Tag and any relevant Client in respect of all Losses suffered or incurred by, awarded against or agreed to be paid by, the Tag arising from or in connection with:
- 11.1.1 any breach by the Supplier of its obligations under this Schedule or the Data Protection Legislation; or

- 11.1.2 the Supplier (or any person acting on its behalf) acting outside or contrary to the processing instructions of the Tag which the Supplier must comply with in accordance with clause 6.1 in respect of the processing of Personal Data.

## **12. MARKET-SPECIFIC DATA PROTECTION TERMS**

- 12.1 Where the UK Data Protection Law (as such term is defined in Annex 5) applies to the processing of Personal Data by the Supplier, the provisions of this Schedule and the provisions of Annex 5 apply to such processing.
- 12.2 Where the Data Protection Legislation of any of the APAC countries applies to the processing of Personal Data by the Supplier, the provisions of this Schedule and the provisions of Annex 6 apply to such processing.

## **13. RIGHTS OF THIRD PARTIES**

A person who is not a party to this Schedule has no rights to enforce any terms of this Schedule by virtue of any Applicable Law relating to third party rights ("**Third Party Rights Legislation**"), including the Singapore Contracts (Rights of Third Parties) Act Chapter 53B and the UK Contracts (Rights of Third Parties) Act 1999 but this does not affect any right or remedy of a third party which exists or is available apart from such Third Party Rights Legislation.

## **14. GENERAL**

- 14.1 This Agreement will be governed by English law, and the parties submit to the exclusive jurisdiction of the courts of England and Wales for all purposes connected with this Agreement, including the enforcement of any award or judgement made under or in connection with it.
- 14.2 Failure by either party to exercise or enforce any rights available to that party or the giving of any forbearance, delay or indulgence shall not be construed as a waiver of that party's rights under this Agreement.
- 14.3 If any term or provision of this Agreement shall be held to be illegal or unenforceable, in whole or in part, under any enactment or rule of law, such term or provision or part shall to that extent be deemed not to form part of this Agreement but the enforceability of the remainder of this Agreement shall not be affected provided, however, that if any term or provision or part of this Agreement is severed as illegal or unenforceable, the parties shall seek to agree to modify this Agreement to the extent necessary to render it lawful and enforceable and as nearly as possible to reflect the intentions of the parties embodied in this Agreement including, without limitation, the illegal or unenforceable term or provision or part.
- 14.4 This Agreement and the documents attached to or referred to in this Agreement shall constitute the entire understanding between the parties as to its subject matter and shall supersede all prior agreements, negotiations and discussions between the parties in respect of the same subject matter. In particular the parties warrant and represent to each other that in entering into this Agreement they have not relied upon any statement of fact or opinion made by the other, its officers, servants or agents which has not been included expressly in this Agreement. Further, each party hereby irrevocably and unconditionally waives any right it may have:
- 14.4.1 to rescind this Agreement by virtue of any misrepresentation; or
- 14.4.2 to claim damages for any misrepresentation whether or not contained in this Agreement; save in each case where such misrepresentation or warranty was made fraudulently.

- 14.5 Notices shall be in writing and shall be sent to the other party marked for the attention of the person at the address set out below. Notices may be sent by first-class mail. Correctly addressed notices sent by first-class mail shall be deemed to have been delivered 72 hours after posting.
- 14.6 This Agreement may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement.

The parties deemed to have signed this Agreement on the date set out in the Master Service Agreement.

### Annex 1 – data protection particulars

The Parties Agree to incorporate and complete Annex 1 & 2 to the main contract with the relevant information as stated therein

<b>Purposes and scope</b>	<i>The Supplier is processing Personal Data for the purpose of delivering to the Tag the Services on behalf of one or more of the Tag's Clients.</i>
<b>Subject matter and nature of processing</b>	<p><i>The subject matter and nature of such processing is as indicated below:</i></p> <p><input type="checkbox"/> Marketing services</p> <p><input type="checkbox"/> Advertising services</p> <p><input type="checkbox"/> Technology services (such as infrastructure, hosting, software)</p> <p><input type="checkbox"/> Other (please specify)</p> <p>.....</p>
<b>Duration</b>	<i>The duration of the processing described herein corresponds to the duration of the Agreement.</i>
<b>Categories of Personal Data processed (including, where applicable, exported)</b>	<p><i>The subject matter of the processing of Personal Data under the Agreement comprises the following data types/categories:</i></p> <p><input type="checkbox"/> Background checks</p> <p><input type="checkbox"/> Browsing information</p> <p><input type="checkbox"/> Contact information</p> <p><input type="checkbox"/> Education and skills</p> <p><input type="checkbox"/> Employment information</p> <p><input type="checkbox"/> Education and skills</p> <p><input type="checkbox"/> Family information</p> <p><input type="checkbox"/> Financial information</p> <p><input type="checkbox"/> Genetic information</p> <p><input type="checkbox"/> Government identifiers</p> <p><input type="checkbox"/> Financial information</p>

	<div> <input type="checkbox"/> Professional experience and affiliations         </div> <div> <input type="checkbox"/> Social media information         </div> <div> <input type="checkbox"/> Travel and expense         </div> <div> <input type="checkbox"/> User account information         </div> <div> <input type="checkbox"/> Workplace welfare         </div> <div> <input type="checkbox"/> Other (please specify)         </div> <div>           .....         </div> <div> <b>Special categories (or other sensitive types) of data</b> </div> <div> <input type="checkbox"/> Racial or ethnic origin         </div> <div> <input type="checkbox"/> Political opinion         </div> <div> <input type="checkbox"/> Religious or philosophical beliefs         </div> <div> <input type="checkbox"/> Trade union membership         </div> <div> <input type="checkbox"/> Genetic data         </div> <div> <input type="checkbox"/> Biometric data         </div> <div> <input type="checkbox"/> Health data         </div> <div> <input type="checkbox"/> A person's sex life or sexual orientation         </div> <div> <input type="checkbox"/> Data relating to criminal convictions         </div>
<b>Categories of Data Subjects</b>	<div> <i>The Personal Data indicated in the row above relates to the following data subjects:</i> </div> <div> <input type="checkbox"/> Consumers         </div> <div> <input type="checkbox"/> Contractors         </div> <div> <input type="checkbox"/> Tag clients' personnel         </div> <div> <input type="checkbox"/> Tag clients' consumers         </div> <div> <input type="checkbox"/> Employees         </div> <div> <input type="checkbox"/> Prospective Employees         </div>

	<input type="checkbox"/> Other (please specify) .....
<b>Frequency of the data transfer to the Supplier</b>	<p><i>[Note: this section should be completed only where personal data is exported and the Transfer Mechanism is selected as "Standard Contractual Clauses". It may otherwise be deleted.]</i></p> <input type="checkbox"/> One-off <input type="checkbox"/> Continuous
<b>Retention period</b>	<p><i>[Note: this section should be completed only where personal data is exported and the Transfer Mechanism is selected as "Standard Contractual Clauses". It may otherwise be deleted. In this section, the parties need to provide the period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period]</i></p>
<b>Specific Restrictions</b>	<p><i>The processing of Personal Data shall be subject to the restrictions described in the Agreement</i></p>
<b>Supplier Data Protection Officer</b>	<p><i>[Insert name and contact details if applicable.]</i></p>

## Annex 2 – Permitted Sub-Processors and Transfers

Permitted Sub-Processors and Transfers						
<p>[Note: Data Protection Legislation (and the new EU Standard Contractual Clauses) require that it is clear to whom and where personal data is transferred and, in particular if there is a transfer from one jurisdiction to another. This table sets out what is agreed by the Tag at the point of signature. The Tag should complete this table in the first instance to indicate which Sub-Processors will process Personal Data and whether any Personal Data will be transferred outside of the EEA or the UK or another country.]</p> <p>The "Mechanism" column sets out any agreed safeguards to enable the transfer of Personal Data overseas in accordance with relevant laws. As examples, transfers of personal data outside of the EEA may require the use of EEA Standard Contractual Clauses or binding corporate rules; transfers of personal data outside of South Korea require the consent of data subjects. No overseas transfers will be able to take place until the relevant mechanism is in force.]</p>						
Sub-Processor name	Contact person's name, position and contact details	Services and description of processing (including subject matter and nature of the processing)	Location/Transfers	Mechanism [Tick relevant box(es) below]	Duration of the processing	Frequency of transfers to this Sub-Processor [Tick relevant box below]
[Set out here the name and registered address of the Sub-Processor]	[If the Sub-Processor has a DPO, this contact should be the Sub-Processor's DPO]	[Set out here the permitted services that they will undertake in relation to Personal Data]	[Set out here the location(s) in which the Sub-Processor will process the Personal Data (including any locations from which the Supplier will access the Personal Data, indicating where and from whom this has been transferred where relevant)]	<input type="checkbox"/> Transfer is to a country, a territory or one or more specified sectors in that country, or to an international organisation that the EU Commission and/or the UK Government and/or another relevant Government has deemed adequate  <input type="checkbox"/> Binding corporate rules  <input type="checkbox"/> EEA Controller to Processor Standard Contractual Clauses  <input type="checkbox"/> Other Controller to Processor Standard Contractual Clauses: [Specify]  <input type="checkbox"/> Consent from data subjects	[Specify]	<input type="checkbox"/> One-off  <input type="checkbox"/> Continuous

### **Annex 3 – Technical and organisational measures**

The Parties agree to comply with Tag Data Security Schedule of the Agreement, which sets out comprehensive Technical and Organisational Security Measures implemented by the Supplier (Data Importer) and with which it will comply.

## Annex 4

### Incorporation of the EEA SCCs

1. Where the EEA SCCs are agreed as required by the parties for a Restricted Transfer:
  - a. The Supplier shall assist the Tag in conducting any required Transfer Impact Assessments in order to ensure the compliance of the Transfer Mechanism with Data Protection Legislation; and
  - b. The EEA SCCs are hereby deemed accepted by the parties and incorporated and read as follows:

EEA SCC clause reference	Interpretation – Processor – Processor Module	Interpretation – Processor – Controller Module
Clause 7 – optional docking clause	Clause is not included	Clause is not included
Clause 9 – use of sub-processors	OPTION 1: SPECIFIC PRIOR AUTHORISATION is chosen and the clause will be read as including “2 weeks” where the EEA SCCs require a specified time period	N/A
Clause 11 - redress	The optional paragraph within clause 11(a) is removed.	The optional paragraph within clause 11(a) is removed
Clause 17 – governing law	The Laws of England and Wales, shall be included into Clause 17 where a Member State is required to be specified	The Laws of England and Wales, and shall be included into Clause 17 where a Member State is required to be specified
18 – choice of forum and jurisdiction	England shall be included into Clause 18 where a Member State is required to be specified	England shall be included into Clause 18 where a Member State is required to be specified
Part A, Annex I – list of parties	For transfers from the Tag to the Supplier, the Tag identified as the data exporter and for transfers from the Supplier to the Tag, the Supplier identified as the data exporter; and  For transfers from the Tag to the Supplier, the Supplier identified as the data importer and for transfers from the Supplier to the Tag, the Tag identified as the data importer.	For transfers from the Tag to the Supplier, the Tag identified as the data exporter and for transfers from the Supplier to the Tag, the Supplier identified as the data exporter; and  For transfers from the Tag to the Supplier, the Supplier identified as the data importer and for transfers from the Supplier to the Tag, the Tag identified as the data importer.
Part B, Annex I – description of transfer	Populated with the relevant details of Annex 1 and Annex 2 of this Schedule	Populated with the relevant details of Annex 1 and Annex 2 of this Schedule
Part C, Annex I – competent supervisory authority	The Information Commissioner Office shall be included where a competent supervisory authority is required to be specified	N/A

Annex II – technical and organisational measures	Populated with the details of Annex 3 of this Schedule	N/A
Annex III – list of sub-processors	Populated with the details of Annex 2 of this Schedule	N/A

2. Where the Swiss Federal Act on Data Protection of June 19, 1992, as amended or replaced (“Swiss FADP”) applies, the EEA SCCs above will apply as follows:
- a. the Swiss Data Protection and Information Commissioner is the exclusive supervisory authority;
  - b. the term “member state” must not be interpreted in such a way as to exclude data subjects of Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 of the EEA SCCs; and
  - c. references to the GDPR in the EEA SCCs shall also include the reference to the equivalent provisions of the Swiss FADP.

## **Annex 5**

### **Compliance with UK Data Protection Law**

Where Standard Contractual Clauses are agreed as required by the Parties for a Restricted Transfer involving any Tag Personal Data that is subject to the UK Data Protection Law:

- The Supplier shall assist the Tag in conducting any required Transfer Impact Assessments in order to ensure the compliance of the Transfer Mechanism with Data Protection Legislation; and
- the EEA SCCs found in Annex 4 to this Schedule are incorporated, as amended by the Information Commissioner's Office International Data Transfer Addendum to the EU Commission Standard Contractual Clauses version B1.0 (the "IDTA") is hereby incorporated into this Schedule as the Transfer Mechanism for any Restricted Transfers of Client Personal Data from the United Kingdom to a Non-Adequate Recipient, as populated by the Addendum to this Annex 5

### **Addendum to Annex 5 ("Addendum")**

#### **Part 1: Tables**

##### **Table 1: Parties and signatures**

Table 1 is populated as follows:

- The details of the Exporter and the Importer are populated with the relevant details of the Client and the Tag (as appropriate for the transfer) \_as found in the Agreement.
- The Key Contact for the Tag is the Data Protection Officer, contactable at [global.privacy@tagww.com](mailto:global.privacy@tagww.com). The Key Contact for the Client is populated with the details of the signatory to the Agreement.
- The signatures to the Agreement to which this Schedule attaches constitute the signatures confirming each party agreeing to be bound by the IDTA.

##### **Table 2: Selected SCCs, Modules and Selected Clauses**

Table 2 is populated as follows:

- The Approved EU SCCs, including the Appendix Information, and with only the following modules, clauses or operational provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum
- The modules and operational clauses in table 2 are populated with the relevant details of Annex 4 of this Schedule.
- For the purposes of Option 4, personal data received from the importer may be combined with personal data collected by the exporter.

##### **Table 3: Appendix Information**

Table 3 is populated as follows:

- The list of parties is populated with the details of the parties found in the Agreement.
- A description of the transfer is populated with the details of the Schedule and of Annex 1 and 2 of the Schedule.
- The technical and organisational measures is populated with the details of Annex 3 of the Schedule.
- The list of Sub-Processors is populated with the details of Annex 2 of this Schedule.

##### **Table 4: Ending this Addendum when the Approved Addendum Changes**

Neither party may end this Addendum is set out in Section 19 of the IDTA.

## Annex 6

### Compliance with Data Protection Legislation in APAC

#### Transfer Mechanism for South Korea

Where a Restricted Transfer set out in clause 6.8.1 would result in the transfer of Personal Data from South Korea to a Non-Adequate Recipient outside South Korea, the only applicable Transfer Mechanism is consent from data subjects.

#### SCCs for transfer of Personal Data from an APAC jurisdiction to a Non-Adequate Recipient

Where a Restricted Transfer set out in clause 6.8.1 would result in the transfer of Personal Data from an APAC jurisdiction to a Non-Adequate Recipient outside such APAC jurisdiction, the Tag may at its option, require the Supplier to enter into SCCs in relation to such Restricted Transfer. The SCCs shall not derogate from any of the Supplier's obligation under this Agreement but shall operate in addition to the Supplier's obligations under this Agreement.

The SCCs include, as applicable:

- (i) the ASEAN Model Contractual Clauses for Cross Border Data Flows ("**ASEAN MCCs**");
- (ii) the Hong Kong Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data ("**HK RMCs**");
- (iii) the New Zealand Model Contract Clauses Agreement ("**NZ Model Agreement**") for Principle 12 of the Privacy Act 2020; and
- (iv) the China Standard Contract for Outbound Transfer of Personal Information ("**China Standard Contract**") issued by the Cyberspace Administration of China