



## Data Processing Addendum

between

Customer  
(**"Data Controller"**)

and

CargoIT | Skandinavien AB  
(**"Data Processor" / "CargoIT"**)

# Table of Contents

.....Error! Bookmark not defined.

- 1. DEFINITIONS.....3
- 2. SCOPE AND APPLICATION OF THIS ADDENDUM.....6
- 3. DATA PROCESSING.....6
- 4. OBLIGATIONS OF THE DATA CONTROLLER .....7
- 5. DURATION; TERMINATION; RETURN OR DELETION OF PERSONAL DATA.....8
- 6. LIABILITY .....8
- 7. AUDITS AND INFORMATION REQUESTS .....8
- 8. APPOINTMENT OF SUBPROCESSORS .....8
- 9. AUTHORIZED AFFILIATES.....9
- 10. STANDARD CONTRACTUAL CLAUSES .....9
- 11. MISCELLANEOUS PROVISIONS.....12
- Schedule 1: Description of the Processing.....14
- Schedule 2: Description of Technical and Organizational Measures .....16
- Schedule 3: Subprocessors .....20
- Schedule 4: Standard Contractual Clauses .....22
- Schedule 5: PRC Personal Information Requirements.....33
- Schedule 6: Taiwan Data Processing Requirements.....36
- Schedule 7: South African Data Processing Requirements.....38
- Schedule 8: Brazil Data Processing Requirements.....41

THIS ADDENDUM is made

**BETWEEN:**

- (1) Customer (the “Data Controller”); and
  - (2) CargolT (the “Data Processor”),
- (each a “Party”, and together the “Parties”).

**WHEREAS:**

1. This Addendum is entered into to ensure adequate safeguards with respect to the protection of privacy and security of Personal Data transferred from the Data Controller to the Data Processor for Processing or accessed by the Data Processor on the authority of the Data Controller for Processing or otherwise received by the Data Processor for Processing on the Data Controller’s behalf.
2. This Addendum forms part of and shall be incorporated in the Agreement or Terms of Use (as applicable) between CargolT and Customer under which CargolT’ Services are offered (“Service Agreement”).

**IT IS AGREED THAT:**

**1. DEFINITIONS**

- 1.1. In this Addendum, the following capitalized terms shall have the following meanings:

|                               |   |
|-------------------------------|---|
| <b>“Affiliate”</b>            | means any entity controlling, controlled by, or under common control of the subject entity. For the purposes of this definition, “control” (including with correlative meanings, the terms “controlled by” and “under common control with”), as used with respect to the subject entity, means the possession, directly or indirectly, of the power to direct or exercise a controlling influence on the management or policies of such entity, whether through the ownership of voting securities, by contract or otherwise; |
| <b>“Australia”</b>            | means the Commonwealth of Australia and each of its states and territories;   |
| <b>“Authorized Affiliate”</b> | means any of Customer Affiliate(s) which (a) is subject to the data protection laws and regulations of the EEA and/or its member states, Switzerland, and/or the UK, and (b) is permitted to use Services pursuant to the Service Agreement;  |
| <b>“CCPA”</b>                 | means the California Consumer Privacy Act;  |
| <b>“Customer”</b>             | means the customer to the Service Agreement;  |
| <b>“Data Controller”</b>      | means the entity that determines the purposes and means of the Processing of Personal Data;   |

|   |  |
|---|--|
| <b>“Data Processor”</b>                       | means the entity that Processes Personal Data on behalf of the Data Controller;  |
| <b>“Data Protection Laws and Regulations”</b> | means all laws and regulations, including all international, national, state and local laws and regulations, such as those of the EEA and its member states, Switzerland, the UK, Australia, and the CCPA and other U.S. and state laws, applicable to the Processing of Personal Data under the Addendum;   |
| <b>“Data Subject”</b>                         | means an identified or identifiable natural person who is the subject of Personal Data;  |
| <b>“DPA”</b>                                  | means this Data Processing Agreement’  |
| <b>“EEA”</b>                                  | means the European Economic Area;  |
| <b>“EU”</b>                                   | means the European Union;  |
| <b>“GDPR”</b>                                 | refers to 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);  |
| <b>“ICO UK Addendum”</b>                      | 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;   |
| <b>“Instruction”</b>                          | means the written instruction, submitted by the Data Controller to the Data Processor, and directing the same to perform a specific action with regard to Personal Data (including depersonalizing, blocking, deletion, making available, etc.);   |
| <b>“Personal Data”</b>                        | means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity; |
| <b>“Personal Data Breach”</b>                 | means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;  |

|  |   |
|--|---|
| <b>"Process/ed/ing"</b>                      | means any operation or set of operations which is performed on the Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;         |
| <b>"Schedule"</b>                            | means the respective schedule(s) annexed to and forming part of this Addendum;  |
| <b>"Services"</b>                            | means Processing of the Personal Data by the Data Processor in connection with and for the purposes of the provision of the services to be provided by the Data Processor to the Data Controller relating to the Service Agreement including as described in <u>Schedule 1</u> to this Addendum;  |
| <b>"Standard Contractual Clauses"/"SCCs"</b> | means the agreement executed by and between Data Controller and Data Processor, attached hereto as <u>Schedule 4</u> pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council;                     |
| <b>"Subprocessor"</b>                        | means any processor engaged by the Data Processor (or by any other Subprocessor of the Data Processor) who agrees to receive from the Data Processor (or from any other Subprocessor of the Data Processor) Personal Data exclusively intended for Processing such Personal Data on behalf of the Data Controller in accordance with its Instructions and the terms of the written subcontract; |
| <b>"Switzerland"</b>                         | means the Swiss Confederation;  |
| <b>"UK"</b>                                  | means the United Kingdom of Great Britain and Northern Ireland;   |
| <b>"UK GDPR"</b>                             | means the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 c. 16;  |
| <b>"U.S."</b>                                | means the United States of America; and   |
| <b>CargoIT</b>                               | means the entity which is a party to the Service Agreement and this Addendum; as determined by the Service Agreement, being CargoIT I Skandinavien AB of Anton Tamms väg 1, SE-194 34, Upplands Väsby, Sweden.  |

1.2. The captions and section headings used are for the purposes of reference and convenience only, are not a part of this Addendum, and shall not be used in construing this Addendum.

- 1.3. Each of CargoIT and the Customer consents to the other's use of electronic acceptance of the terms of this Amendment, which shall be considered to be an original binding signature.
- 1.4. Unless the context otherwise requires, words denoting the singular shall include the plural and vice versa, references to any gender shall include all other genders and references to persons shall include bodies corporate, unincorporated associations and partnerships, in each case whether or not having a separate legal personality. References to the word "include" or "including" are to be construed without limitation.
- 1.5. References to recitals, schedules and clauses are to recitals and schedules to and clauses of this Addendum unless otherwise specified and references within a schedule to paragraphs are to paragraphs of that schedule unless otherwise specified.
- 1.6. References in this Addendum to any statute, statutory provision or law include a reference to the statute or statutory provision or the law as from time to time amended, extended or re-enacted. Any reference to "writing" or "written" includes faxes and any non-transitory form of visible reproduction of words (like emails), unless expressly indicated to the contrary.

## 2. SCOPE AND APPLICATION OF THIS ADDENDUM

- 2.1. The subject-matter, nature and purpose as well as the type of Personal Data and the categories of Data Subjects affected are set out in [Schedule 1](#) to this Addendum.
- 2.2. This Addendum shall apply, in relation to the Services, to:
  - 2.2.1. all Personal Data sent from the date of this Addendum by or on behalf of the Data Controller to the Data Processor for Processing;
  - 2.2.2. all Personal Data accessed by the Data Processor on the authority of the Data Controller for Processing from the date of this Addendum; and
  - 2.2.3. all Personal Data otherwise received by the Data Processor for Processing on the Data Controller's behalf.

## 3. DATA PROCESSING

The Data Processor agrees to Process the Personal Data to which this Addendum applies in accordance with the terms and conditions set out in this Addendum, and in particular the Data Processor agrees:

- 3.1. not to Process the Personal Data for any purpose other than the specific purpose of performing the Services set forth in this Addendum. The Data Processor also agrees it will not sell or rent the Personal Data for any purpose;
- 3.2. to Process the Personal Data only on behalf of the Data Controller and at all times in compliance with the Data Controller's Instructions based on this Addendum. This Addendum and the Service Agreement are Data Controller's complete and final documented Instructions at the time of execution of the Service Agreement to the Data Processor for the Processing of Personal Data. Any additional or alternate Instructions must be agreed upon separately. Instructions orally given shall be promptly confirmed in writing by the Data Controller. If the Data Processor cannot provide such compliance for whatever reasons, it agrees to promptly notify the Data Controller of its inability to comply, unless laws applicable to the Data Processor prohibit such information on important grounds of public interest. Where the Data Processor believes that compliance with any Instructions by the Data Controller would result in a violation of Data Protection Laws and Regulations, the Data Processor shall notify the Data Controller thereof in writing without delay;
- 3.3. that within the Data Processor's area of responsibility, the Data Processor shall structure its internal corporate organization to ensure compliance with the specific requirements of the protection of Personal Data. The Data Processor shall take appropriate technical and organizational measures to adequately protect Personal Data Processed on behalf of the Data Controller against misuse and loss in accordance with the requirements of Data Protection Laws and Regulations. An overview of the technical and organizational measures agreed at the time of execution of this Addendum between

the Parties has been attached as Schedule 2 to this Addendum. The Data Processor regularly monitors compliance with these measures. The Data Processor may change the technical and organizational measures implemented to adequately protect the Data Controller's Personal Data against misuse and loss as long as such changes will not materially decrease the overall security of the Services during the subscription term;

- 3.4. that persons entrusted with the Processing of the Data Controller's Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- 3.5. not to divulge the Personal Data whether directly or indirectly to any person, firm or company or otherwise without the express prior written consent of the Data Controller except to those of the Data Processor's partners, officers, directors, employees, accountants, attorneys, independent contractors, temporary employees, affiliates, agents or any other representatives that may from time to time be employed, retained by, working for, or acting on behalf of, the Data Processor with a bona fide need to have access to such Personal Data (collectively, "Representatives") and Subprocessors who are engaged in the Processing of the Personal Data and are subject to the obligations referred to in clause 3.3, or except as may be required by any law or regulation applicable to the Data Processor, its Representatives or Subprocessors;
- 3.6. that it will notify the Data Controller in writing and without undue delay about:
  - 3.6.1. a Personal Data Breach. Such notification shall include, taking into account the nature of the Processing, and the information available to the Data Processor, information relevant to reasonably assist the Data Controller in ensuring compliance with its own notification obligations under Data Protection Laws and Regulations. In so far as it is not possible to provide all relevant information at the same time, the Data Processor may provide the information in phases without further undue delay;
  - 3.6.2. any request received directly from a Data Subject without responding to that request, unless it has been otherwise authorized to do so in writing by the Data Controller;
- 3.7. Taking into account the nature of the Processing and, at the cost of the Data Controller, to reasonably assist the Data Controller by appropriate technical and organizational measures, insofar as this is reasonably possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights laid down by Data Protection Laws and Regulations;
- 3.8. At the cost of the Data Controller, to make available to the Data Controller all information reasonably necessary to demonstrate compliance with the obligations laid down in this Addendum and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller as set forth in clause 7;
- 3.9. That any Processing services carried out by a Subprocessor will be carried out in accordance with clause 8;
- 3.10. That the Data Processor has appointed a data protection officer to the extent this is required by Data Protection Laws and Regulations. The Data Processor will provide the contact details of the appointed person upon request of the Data Controller; and
- 3.11. At the cost of Data Controller to reasonably assist the Data Controller in ensuring compliance with the obligation to carry out data protection impact assessments and prior consultations with supervisory authorities, taking into account the nature of the Processing and the information available to the Data Processor.

#### **4. OBLIGATIONS OF THE DATA CONTROLLER**

The Data Controller agrees and warrants that any disclosure of Personal Data made by or on behalf of it to the Data Processor is made with the Data Subject's consent or is otherwise lawful.

## 5. DURATION; TERMINATION; RETURN OR DELETION OF PERSONAL DATA

This Addendum will become effective when the Parties' Service Agreement into which this Addendum has been incorporated enters into effect. This Addendum will terminate automatically upon the later of (a) termination or expiry of the Data Processor's obligations in relation to the Services or (b) termination of Processing of the Personal Data by the Data Processor. On termination of this Addendum, the Data Processor shall return to the Data Controller or delete, at the Data Controller's choice, all Personal Data Processed on behalf of the Data Controller, unless applicable law requires storage of the Personal Data. Upon the request of the Data Controller, the Data Processor shall confirm compliance with such obligations in writing.

## 6. LIABILITY

The Parties agree that the limitations of liability set forth in the Service Agreement apply to any violation of the provisions of this Addendum or any damage which may result from the Data Processor's or any Subprocessor's non-compliance with Data Protection Laws and Regulations. Nothing in this clause will affect the remaining terms of the Service Agreement relating to liability, including any specific exclusions from any limitation of liability.

## 7. AUDITS AND INFORMATION REQUESTS

The Data Controller may during regular business hours without unreasonably interfering with the Data Processor's business operations, and after a reasonable prior notice, personally audit Data Processor, or appoint a third-party auditor, who is subject to confidentiality obligations and not acting as a competitor of the Data Processor, to carry out such audit at the Data Controller's sole cost. The Data Controller agrees to audit CargolT not more than once per year and only after a reasonable prior notice, ie. not less than thirty (30) days, unless there are indications of non-compliance or in case the audit is required by a decision of a data protection supervisory authority, a court or under applicable Data Protection Laws and Regulations following a Personal Data Breach at the Data Processor concerning the Personal Data of the Data Controller. Before the initiation of any such on-site audit, the Data Controller and the Data Processor shall mutually agree upon the scope, timing, and duration of the audit. The Data Processor shall, upon request and within a reasonable time, provide the Data Controller with relevant information to assist any audit of the Processing governed by this Addendum. In deciding on an audit, the Data Controller shall take into account relevant certifications held or audit reports provided by the Data Processor. The Data Controller ensures and is responsible that the results of the audit report are kept confidential, unless disclosure is required by a data protection supervisory authority, a court or applicable Data Protection Laws and Regulations. The Data Processor will charge the Data Controller for the reasonable costs incurred with respect to responding to information requests and assisting with audits.

## 8. APPOINTMENT OF SUBPROCESSORS

- 8.1. The Data Controller hereby consents to and generally authorizes the engagement of Subprocessors by the Data Processor. Currently, and depending on the choice of Services, the Data Processor has engaged the Subprocessor(s) set forth in Schedule 3 whose engagement is hereby authorized by the Data Controller.
- 8.2. The Data Processor shall provide notification of a new Subprocessor to the Data Controller before authorizing the new Subprocessor to Process Personal Data in connection with the provision of the Services. In order to exercise its right to object to Data Processor's use of a new Subprocessor, the Data Controller shall notify the Data Processor promptly in writing within ten (10) days of receipt of the Data Processor's notice. In the event the Data Controller objects to a new Subprocessor, and that objection is duly substantiated and not unreasonable, the Data Processor will use reasonable efforts to make available to the Data Controller a change in the Services or, in the alternative, recommend a commercially reasonable change to Data Controller's configuration or use of the Services to avoid Processing of Personal Data by the contested new Subprocessor without unreasonably burdening the Data Controller. If the Data Processor is unable to make available such change within a reasonable



period of time, which shall not exceed thirty (30) days, the Data Controller may terminate the relevant portion(s) of the Services which cannot be provided by the Data Processor without the use of the contested new Subprocessor by providing written notice to the Data Processor.

- 8.3. Any such Processing by a Subprocessor shall be done pursuant to a written agreement that is no less restrictive than this Addendum. Such written agreement will require the Subprocessor to Process the Personal Data only to provide the Services specified in the written agreement and not Process the Personal Data for its own purposes.
- 8.4. No Processing by a Subprocessor will release the Data Processor from its responsibility for its obligations under this Addendum, and the Data Processor will be fully liable to the Data Controller for the work and activities of each of its Subprocessors subject to the limitations of the Service Agreement.

## 9. AUTHORIZED AFFILIATES

The Parties acknowledge and agree that, by executing the Service Agreement, the Data Controller enters into the Addendum, in the name and on behalf of its Authorized Affiliates (to the extent any such Affiliates are authorized under the applicable Service Agreement), thereby establishing a separate Addendum between the Data Processor and each such Authorized Affiliate subject to the provisions of the Service Agreement and this clause 9. Each Authorized Affiliate agrees to be bound by the obligations under this Addendum and, to the extent applicable, the Service Agreement.

The Data Controller represents and warrants that it has been duly authorized by its Authorized Affiliates to enter into this Addendum in the name and on behalf of its Authorized Affiliates.

## 10. STANDARD CONTRACTUAL CLAUSES

- 10.1. In the course of the provision of Services under the Service Agreement by the Data Processor, it will be necessary to transfer Personal Data from the Data Controller or any Authorized Affiliate to the Data Processor and its Subprocessors located in the United States of America.
- 10.2. For the purposes of the data transfers referred to in clause 10.1, the SCCs shall form an integral part of this Addendum and apply as further specified in the following clauses 10.3 to 10.17, which contain operative provisions for the implementation of the SCCs, to the
  - (a) Data Controller; and
  - (b) Authorized Affiliates of the Data Controller,
 if either of the aforementioned entities is subject to the Data Protection Laws and Regulations of the EU, the EEA and/or its member states, Switzerland and/or the UK. For the purposes of the SCCs, the ICO UK Addendum and this clause 10, the aforementioned entities are individually or collectively the **"Data Exporter"**, whereas CargoIT is the **"Data Importer"**.
- 10.3. For the purposes of clauses 8.1(a) and 8.8 of the SCCs, clause 3 of this Addendum and the Service Agreement are the Data Exporter's complete and final documented instructions at the time of execution of the Service Agreement to CargoIT for the Processing of Personal Data and include onward transfers to third parties, including to Subprocessors, located outside the EU/EEA for the purpose of the performance of the Services. Any additional or alternate instructions must be consistent with the terms of this Addendum and the Service Agreement.
- 10.4. For the purposes of clauses 8.5 and 16(d) of the SCCs, the Parties agree that the certification of deletion of Personal Data shall be provided by CargoIT to the Data Exporter only upon written request.
- 10.5. For the purposes of clause 8.6(a) of the SCCs, the Data Exporter is solely responsible for making an independent determination as to whether the technical and organisational measures set forth in Annex II to the SCCs meet its requirements. The Data Exporter agrees that at the time of execution of the Service Agreement, 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 organizational measures taken by CargoIT provide a level of security appropriate to the risk with respect to the Personal Data.

- 10.6. For the purposes of clause 8.9(a)-(c) of the SCCs, CargoIT shall handle Data Exporter's requests for information in accordance with clause 3.7 of this Addendum.
- 10.7. For the purposes of clauses 8.9(c)-(e) of the SCCs, any audit shall be carried out in accordance with clause 7 of this Addendum.
- 10.8. For the purposes of clause 9.a of the SCCs, the following shall apply:
  - 10.8.1. CargoIT has the Data Exporter's general authorization to engage Subprocessors in accordance with clause 8 of this Addendum. A current list of Subprocessors is attached as Schedule 3 to this Addendum. CargoIT shall inform the Data Exporter of any changes to Subprocessors following the procedure set out in clause 8 of this Addendum.
  - 10.8.2. Where CargoIT enters into Module 3 of the SCCs (governing transfers of Personal Data between Data Processors) with a Subprocessor in connection with the provision of the Services, the Data Exporter hereby grants CargoIT and its Affiliates authority to provide a general authorization on behalf of the Data Exporter 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 such Subprocessors.
- 10.9. For the purposes of clause 11 of the SCCs, and subject to clause 3.6 of this Addendum, CargoIT shall inform Data Subjects on its website of a contact point authorized to handle complaints. CargoIT shall inform the Data Exporter 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 shall without undue delay communicate the complaint or dispute to the Data Exporter. CargoIT shall not have any further obligation to handle the request, unless otherwise agreed with the Data Exporter in each individual case.
- 10.10. For the purposes of clause 12 of the SCCs, the following shall apply:
  - 10.10.1. CargoIT's liability under clause 12(a) of the SCCs shall be subject to the limitations of the Service Agreement.
  - 10.10.2. CargoIT's liability under clause 12(b) of the SCCs shall be limited to any damage caused by its Processing where it has not complied with its obligations under the GDPR specifically directed to Data Processors, or where it has acted outside of or contrary to lawful Instructions of the Data Exporter, as specified in Article 82(2) GDPR.
  - 10.10.3. CargoIT shall be exempt from liability under clause 10.10.2 of this Addendum if it proves that it is not in any way responsible for the event giving rise to the damage pursuant to Article 82(3) GDPR.
- 10.11. For the purposes of clause 13 of the SCCs, the following shall apply:
  - 10.11.1. Where the Data Exporter is established in an EU member state, the supervisory authority with responsibility for ensuring compliance by the Data Exporter with the GDPR as regards the data transfer shall act as competent data protection supervisory authority.
  - 10.11.2. Where 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 Article 3(2) and has appointed a representative pursuant to Article 27(1) GDPR, the supervisory authority of the EU member state in which the representative within the meaning of Article 27(1) GDPR is established shall act as competent data protection supervisory authority.
  - 10.11.3. Where 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 Article 3(2) without however having to appoint a representative pursuant to Article 27(2) GDPR, the Hamburg Commissioner for Data Protection and Freedom of Information shall act as competent data protection supervisory authority.
- 10.12. For the purposes of clause 15(1)(a) of the SCCs, the following shall apply:
  - 10.12.1. The Data Importer shall notify the Data Exporter (only) and not the Data Subject(s) in each and every

case it either

- (a) 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 pursuant to the SCCs; or
- (b) Becomes aware of any direct access by public authorities to Personal Data transferred pursuant to the SCCs in accordance with the laws of the country of destination.

10.12.2. The Data Exporter shall be solely responsible for promptly notifying the Data Subject(s) as necessary.

10.13. The governing law for the purposes of clause 17 of the SCCs shall be the law that applies to the Service Agreement. If the Service Agreement is not governed by an EU member state law, the SCCs will be governed by the laws of Germany.

10.14. For the purposes of clause 18(b) of the SCCs, the courts of Germany shall have exclusive jurisdiction to resolve any dispute arising from the SCCs.

10.15. The Appendix to the SCCs are as follows:

- (a) The contents of section 1 of Schedule 1 to this Addendum shall form Annex I.A to the SCCs.
- (b) The contents of section 2 of Schedule 1 to this Addendum shall form Annex I.B to the SCCs.
- (c) The contents of section 3 of Schedule 1 to this Addendum shall form Annex I.C to the SCCs.
- (d) The contents of Schedule 2 to this Addendum shall form Annex II to the SCCs.
- (e) The contents of Schedule 3 to this Addendum shall form Annex III to the SCCs.

10.16. In case of any transfers of Personal Data governed by Data Protection Laws and Regulations of Switzerland, the Parties agree that the SCCs will apply to such transfers in accordance with clauses 10.3 to 10.14 of this Addendum as further specified below:

- (a) General and specific references in the SCCs to the GDPR, EU or EU member state law shall have the same meaning as the equivalent reference in the Data Protection Laws and Regulations of Switzerland;
- (b) For the purposes of clause 13 of the SCCs, the Swiss Federal Data Protection and Information Commissioner shall act as competent data protection supervisory authority insofar as the relevant data transfer is (also) governed by Data Protection Laws and Regulations of Switzerland if the Data Exporter is established in Switzerland or otherwise falls within the territorial scope of Data Protection Laws and Regulations of Switzerland;
- (c) For the purposes of clause 18(b) of the SCCs, the courts of Switzerland shall have exclusive jurisdiction to resolve any dispute arising from the SCCs as specified in this section;
- (d) For the purposes of clause 18(c) of the SCCs, the term "Member State" shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland); and
- (e) The SCCs also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Data Protection Laws and Regulations of Switzerland until such laws are amended to no longer apply to a legal entity.

10.17. In case of any transfers of Personal Data governed by the UK GDPR, the Parties hereby enter into the ICO UK Addendum and its alternative part 2 mandatory clauses, which shall form an integral part of this Addendum. The Parties agree that the SCCs apply to such transfers in accordance with clauses 10.3 to 10.15 of this Addendum, and as amended by the mandatory clauses of the ICO UK Addendum. In accordance with 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 in this Addendum:

- (a) The "start date" for the purposes of part 1 of the ICO UK Addendum is the execution date of Schedule 1 by the Data Controller as specified in clause 10.18 of this Addendum;

- (b) “The parties” for the purposes of part 1 of the ICO UK Addendum are CargolT as the Data Importer and the Data Controller and its Authorized Affiliates as the Data Exporter as further specified in clause 10.2 of this Addendum 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 sections B of [Schedule 1](#);
  - (d) The “Addendum SCCs” for the purposes of part 1 of the ICO UK Addendum are the SCCs as specified in clauses 10.3 to 10.15 of this Addendum;
  - (e) The “Appendix Information” for the purposes of part 1 of the ICO UK Addendum is the information included in [Schedule 1](#) to [Schedule 3](#) as specified in clause 10.15 of this Addendum.
  - (f) For the purposes of part 1 of the ICO UK Addendum, the Data Importer may end the ICO UK Addendum under the conditions set out in section 19 of the ICO UK Addendum.
- 10.18. Signing the Service Agreement constitutes signature of Section A of Schedule 1 by the Data Controller in its own name and in the name and on behalf of its Authorized Affiliates and shall be deemed to constitute signature and acceptance of the SCCs, and to the extent applicable, the ICO UK Addendum, both as specified in this clause 10. By the Data Controller entering into the SCCs and, to the extent applicable, the ICO UK Addendum in the name and on behalf of Authorized Affiliates, such Authorized Affiliates (to the extent any such Affiliates are authorized under the applicable Service Agreement) shall become a party to the SCCs and, to the extent applicable, the ICO UK Addendum as additional Data Exporter/s under [Schedule 1](#) of this Addendum, subject to the provisions of this Addendum and this clause 10. Each Authorized Affiliate agrees to be bound by the obligations under the SCCs and, to the extent applicable, the ICO UK Addendum, both as specified in this clause 10. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the SCCs and, to the extent applicable, the ICO UK Addendum, both as specified in this clause 10, and any violation of the terms and conditions of the SCCs and, to the extent applicable, the ICO UK Addendum by an Authorized Affiliate shall be deemed a violation by the Data Controller.
- 10.19. The Data Controller represents and warrants that it has been duly authorized by its Authorized Affiliates to enter in the name and on behalf of its Authorized Affiliates into the SCCs and to the extent applicable the ICO UK Addendum, both as specified in this clause 10.

## 11. MISCELLANEOUS PROVISIONS

- 11.1. Amendments or additions to this Addendum must be made in writing to be effective. This shall also apply to amendments of this written form requirement. The written form requirement in this clause does not include faxes or any non-transitory form of visible reproduction of words (like emails).
- 11.2. Should any provision of this Addendum be or become invalid, this shall not affect the validity of the remaining terms. The Parties shall in such an event be obliged to cooperate in the creation of terms which achieve such legally valid result as comes closest commercially to that of the invalid provision. The above shall apply accordingly to the closing of any gaps in the Addendum.
- 11.3. Any Data Processor obligations arising from statutory provisions or according to a judicial or regulatory decision shall remain unaffected by this Addendum.
- 11.4. This Addendum shall not replace any comparable or additional rights relating to Processing of Personal Data of the Data Controller contained in the Service Agreement. In the event of any conflict or inconsistency between this Addendum and the Service Agreement, this Addendum shall prevail.
- 11.5. In the event of any conflict or inconsistency between this Addendum and the SCCs, the latter shall prevail.
- 11.6. In the event of any conflict or inconsistency between the SCCs and the ICO UK Addendum, the latter shall prevail, except where (and in so far as) the inconsistent or conflicting terms of the SCCs provide greater protection for Data Subjects, in which case those terms will override the ICO UK Addendum.
- 11.7. This Addendum shall be governed by the same law that is governing the Service Agreement between the Parties, except for the SCCs which shall be governed by the law applicable pursuant to clause 17

of SCCs and 10.13 of this Addendum as well as for any data transfers governed by the UK GDPR clause 10.17 of this Addendum in connection with section 15(m) of the ICO UK Addendum.

**List of Schedules:**

- Schedule 1: Description of the Processing
- Schedule 2: Description of Technical and Organizational Measures
- Schedule 3: Subprocessors
- Schedule 4: Standard Contractual Clauses
- Schedule 5: PRC Personal Information Requirements
- Schedule 6: Taiwan Data Processing Requirements
- Schedule 7: South African Data Processing Requirements
- Schedule 8: Brazil Data Processing Requirements

## Schedule 1: Description of the Processing

### 1. LIST OF PARTIES

#### 1.1. Data Exporter(s)

Customer and its Authorized Affiliates, as defined in the Service Agreement.

(incl. official registration number/company number/similar identifier):

Activities relevant to the data transferred under these Clauses: Performance of the Services pursuant to the Service Agreement and as further described in this Addendum.

Role (controller/processor): For the purposes of the Standard Contractual Clauses set out in Schedule 4 to this Addendum, Customer and/or its Authorized Affiliate is acting as a Data Controller.

#### 1.2. Data Importer(s)

Name: CargolT

Contact person's name, position and contact details: [privacyofficer@wisetechglobal.com](mailto:privacyofficer@wisetechglobal.com)

Activities relevant to the data transferred under these Clauses: Performance of the Services pursuant to the Service Agreement and as further described in this Addendum.

Role (controller/processor): For the purposes of the Standard Contractual Clauses set out in Schedule 4 to this Addendum, CargolT is acting as a Data Processor.

### 2. DESCRIPTION OF THE PROCESSING

#### 2.1. Categories of data subjects whose personal data is transferred

The Personal Data transferred concern the following categories of Data Subjects:

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

#### 2.2. Categories of personal data transferred

The Personal Data transferred concern the following categories of 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

- Disclosed Information (from third parties, e.g. Credit Reference Agencies or from Public Directories).

2.3. **Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved\***

Nil

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

Data is transferred on an ongoing and continuous basis.

2.5. **Nature and purpose of the processing**

As set forth in the Service Agreement between the Parties, as well as any appendices thereto.

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

Unless an alternate period is required by applicable local law or regulation, upon the earlier of: 1) the scheduled tear down of the applicable database(s) as a result of termination of the Service Agreement; or 2) the data exporter providing written confirmation to the data importer that the data exporter(s) no longer requires the data to be retained.

2.7. **Transfers to (sub-)processors: Subject matter, nature and duration of the processing**

As set forth in the Service Agreement between the Parties, as well as any appendices thereto.

**3. COMPETENT SUPERVISORY AUTHORITY**

The Hamburg Commissioner for Data Protection and Freedom of Information

## Schedule 2: Description of Technical and Organizational Measures

Description of the technical and organisational security measures implemented by the data importer:

### **Confidentiality (Article 32(1) lit. (b) GDPR)**

- Physical Access Control  
No unauthorised access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems
- Electronic Access Control  
No unauthorised use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media
- Internal Access Control (permissions for user rights of access to and amendment of data)  
No unauthorised Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorisation concept, need-based rights of access, logging of system access events
- Isolation Control  
The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing; and
- Pseudonymization (Article 32 (1)(a) GDPR; Article 25 (1) GDPR)  
The processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.

### **Integrity (Article 32(1) lit. (b) GDPR)**

- Data Transfer Control  
No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature; and
- Data Entry Control  
Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management.

### **Availability and Resilience (Article 32(1) lit. (b) GDPR)**

- Availability Control  
Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning; and
- Rapid Recovery (Article 32(1) lit. (c) GDPR).



**Procedures for regular testing, assessment and evaluation (Article 32(1) lit. (d) GDPR; Article 25(1) GDPR)**

- Data Protection Management;
- Incident Response Management;
- Data Protection by Design and Default (Article 25(1) GDPR);
- Order or Contract Control ; and
- No third party data processing as per Article 28 GDPR without corresponding instructions from the Customer, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.

**Security measures**

1. Data importer/sub-processor has implemented and shall maintain a security program in accordance with industry standards.
2. More specifically, data importer/sub-processor's security program shall include:

**Access Control of Processing Areas**

Data importer/sub-processor implements suitable measures in order to prevent unauthorised persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the personal data are processed or used, including:

- Establishing security areas;
- Protection and restriction of access paths;
- Establishing access authorisations for employees and third parties, including the respective documentation;
- All access to the data centre where personal data are hosted is logged, monitored, and tracked; and
- The data centre where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

**Access Control to Data Processing Systems**

Data importer/sub-processor implements suitable measures to prevent their data processing systems from being used by unauthorized persons, including:

- Use of adequate encryption technologies;
- Identification of the terminal and/or the terminal user to the data importer/sub-processor and processing systems;
- Automatic temporary lock-out of user terminal if left idle, identification and password required to reopen;
- Automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts (alerts); and
- All access to data content is logged, monitored, and tracked.

### **Access Control to Use Specific Areas of Data Processing Systems**

Data importer/sub-processor commits that the persons entitled to use their data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- Employee policies and training in respect of each employee's access rights to the personal data;
- Monitoring capability in respect of individuals who delete, add or modify the personal data;
- Release of data only to authorised persons, including allocation of differentiated access rights and roles; and
- Use of adequate encryption technologies; and
- Control of files, controlled and documented destruction of data.

### **Availability Control**

Data importer/sub-processor implements suitable measures to ensure that personal data are protected from accidental destruction or loss, including:

- Infrastructure redundancy; and
- Backup is stored at an alternative site and available for restore in case of failure of the primary system.

### **Transmission Control**

Data importer/sub-processor implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- Use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels; and
- As far as possible, all data transmissions are logged, monitored and tracked.

### **Input Control**

Data importer/sub-processor implements suitable input control measures, including:

- An authorisation policy for the input, reading, alteration and deletion of data;
- Authentication of the authorised personnel;
- Protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- Utilisation of unique authentication credentials or codes (passwords);
- Providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked;
- Automatic log-off of user sessions that have not been used for a substantial period of time;
- Proof established within data importer/sub-processor's organization of the input authorisation; and
- Electronic recording of entries.

### **Separation of Processing for different Purposes**

Data importer/sub-processor implements suitable measures to ensure that data collected for different purposes can be processed separately, including:

- Access to data is separated through application security for the appropriate users;
- Modules within the data importer/sub-processor's data base separate which data is used for which purpose, i.e. by functionality and function;
- At the database level, data is stored in separate databases for each customer with credentials that only access individual databases; and
- Interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

### **Documentation**

Data importer/sub-processor will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Data importer/sub-processor shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organisational measures set forth in this Schedule 2.

### **Monitoring**

Data importer/sub-processor shall implement suitable measures to monitor access restrictions to data importer/sub-processor's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by various measures including:

- Individual appointment of system administrators;
- Adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for at least six months;
- Yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by the data importer/sub-processor and applicable laws;
- Keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to data exporter upon request.

### Schedule 3: Subprocessors

The Data Controller has authorized the use of the following Subprocessors through the WiseTech Global Limited corporate Group in which CargoIT is a member:

| Company  | Address   | Service description  | Duration of processing  |
|--|---|--|---|
| Affiliates of the Data Importer listed in Internal sub-processors data centre(s) table below | Refer to Internal sub-processors data centre(s) table below   | Data centres   | For the term of Service Agreement and until tear down of Data Exporter's databases is complete  |
| Microsoft Ireland Operations Limited<br><br>Microsoft Pty Ltd                                | C/o Microsoft Operations Pte Ltd<br>Dept. 551, Volume Licensing, 82 Cecil Street, #13-01 Frasers Tower, Singapore 069547 Republic of Singapore<br><br>1 Epping Road, North Ryde NSW 2113, Australia | Exchange - email<br><br>SharePoint - collaboration tools<br><br>Microsoft Teams - collaboration tools<br><br>Defender ATP - threat protection<br><br>Azure -IaaS, PaaS, SaaS | For the term of Service Agreement and until tear down of Data Exporter's databases is complete  |
| Proofpoint Inc.  | 892 Ross Drive, Sunnyvale, CA 94085, USA  | Email Filtering/quarantine   | For the term of Service Agreement and until tear down of Data Exporter's databases is complete, however, duration of retention of any particular email is two weeks following receipt of each quarantined email |
| Iron Mountain Australian Group Pty Ltd   | Australia Headquarters<br><br>465 Plummer St,<br><br>Port Melbourne VIC 3207  | Off Site Storage   | For the term of Service Agreement and until expiry of retention period required thereafter  |
| Aryaka Networks, Inc.  | 1800 Gateway Drive, Suite 200, San Mateo, CA 94404, USA   | Network acceleration services over the public internet   | For the term of Service Agreement and until tear down of Data Exporter's databases is complete  |

**Internal Sub-Processors**

| Company Name              | Country   | Address   |
|---------------------------|-----------|---|
| WiseTech Global Limited   | Australia | Unit 3a, 72 O’Riordan Street, Alexandria NSW, Australia       |
| WiseTech Global (US) Inc. | USA       | 1051 East Woodfield Road, Schaumburg IL 60173, USA            |
| CargoWise GmbH            | Germany   | c/o Softship GmbH, Notkestraße 13-15, 22607, Hamburg, Germany |

## Schedule 4: Standard Contractual Clauses

### (Module Two: Transfer Controller to Processor)

#### SECTION I

##### Clause 1

###### Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.
- (b) The Parties:
  - i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
  - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

##### Clause 2

###### Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

##### Clause 3

###### Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - ii. Clause 8.1(b), 8.9(a), (c), (d) and (e);
  - iii. Clause 9(a), (c), (d) and (e);

- iv. Clause 12(a), (d) and (f);
  - v. Clause 13;
  - vi. Clause 15.1(c), (d) and (e);
  - vii. Clause 16(e);
  - viii. Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679

#### **Clause 4**

##### **Interpretation**

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

#### **Clause 5**

##### **Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

#### **Clause 6**

##### **Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B

#### **Clause 7 - Optional**

##### **Docking clause**

*(Intentionally left blank.)*

## **SECTION II – OBLIGATIONS OF THE PARTIES**

#### **Clause 8**

##### **Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

##### **8.1. Instructions**

- (a) The data importer shall process the personal data only on documented instructions from the

data exporter. The data exporter may give such instructions throughout the duration of the contract.

- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

## 8.2. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

## 8.3. Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

## 8.4. Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

## 8.5. Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

## 8.6. Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of



security.

- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

#### 8.7. Sensitive data

Where the transfer involves personal data revealing 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 (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

#### 8.8. Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

#### 8.9. Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data

importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

## Clause 9

### Use of sub-processors

- (a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least within ten (10) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

## Clause 10

### Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data

subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

## **Clause 11**

### **Redress**

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - v. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - vi. refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

## **Clause 12**

### **Liability**

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the

data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### Clause 13

#### Supervision

- (a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.  
[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.  
[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.
- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

## *SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES*

### Clause 14

#### Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards<sup>12</sup>
  - iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply

## Clause 15

### Obligations of the data importer in case of access by public authorities

#### 15.1. Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - 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 pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination;

such notification shall include all information available to the importer.

- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

#### 15.2. Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## SECTION IV – FINAL PROVISIONS

### Clause 16

#### Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

- i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
- ii. the data importer is in substantial or persistent breach of these Clauses; or
- iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

## **Clause 17**

### **Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Hamburg, Germany

## **Clause 18**

### **Choice of forum and jurisdiction**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Hamburg, Germany.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX**

**ANNEX I**

*(Please refer to Schedule 1 to this Addendum.)*

**ANNEX II – TECHNICAL AND ORGANISATIONAL MEASURES  
INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO  
ENSURE THE SECURITY OF THE DATA**

*(Please refer to Schedule 2 to this Addendum.)*

**ANNEX III – LIST OF SUB-PROCESSORS**

*(Please refer to Schedule 3 to this Addendum.)*

\* \* \*



## Schedule 5: PRC Personal Information Requirements

This Schedule 5 applies to Customers who are Processing Personal Information in China, or are not domiciled in China but Processing Personal Information of the Data Subjects in China for (i) providing products and services to such Data Subjects; or (ii) analyzing or evaluating behaviour of such Data Subjects. In terms of the Service Agreement, the Customer (as the Data Exporter) may be required to transfer Personal Information to WTG entities (as the Data Importer), which entities may be situated outside of China in order to, amongst other things, carry out the services in terms of the Service Agreement. The location of the storage of the Personal Information outside of China is Australia, Europe and the United States of America.

In order to ensure adequate safeguards for the cross-border transfer of the Personal Information in accordance with the provisions of PIPL, the Parties agree that the Customer shall be entitled to transfer Personal Information to WTG, and WTG shall be entitled to receive and Process the Personal Information, subject to the terms and conditions set out in this Schedule 5 as read together with this DPA.

This Schedule 5 and DPA shall be read and interpreted in the light of the provisions of PIPL and shall not be interpreted in a way that conflicts with rights and obligations provided for in PIPL. In the event of a contradiction between the DPA and this Schedule 5, this Schedule 5 shall prevail.

### 1. DEFINITIONS

For the purposes of this Schedule 5, the following words will have the following meanings and cognate expressions shall have corresponding meanings:

- 1.1 "Competent Supervisory Authority" means the authorities performing personal information protection duties as specified in PIPL;
- 1.2 "Data Exporter" means the Customer, who transfers Personal Information of Data Subjects in China to the Data Importer;
- 1.3 "Data Importer" means the applicable WTG entity, who receives Personal Information from the Data Exporter for Processing in accordance with the terms of this Schedule 5;
- 1.4 "Data Subject" means a natural person to whom the Personal Information relates;
- 1.5 "Entrusted Party" means an individual or organization who Processes Personal Information on behalf of and for the purpose of the Personal Information Processor;
- 1.6 "Personal Information" has the meaning of "personal information" as defined in PIPL, being information relating to an identified or identifiable natural person as electronically or otherwise recorded, excluding information that has been anonymized; and for the avoidance of doubt, "Personal Information" shall include "Sensitive Personal Information";
- 1.7 "PIPL" means the PRC Personal Information Protection Law, including any Regulations, Standards, or other interpretative instruments promulgated or made thereunder, as amended from time to time;
- 1.8 "Processing" or "Process" has the meaning of "processing" as defined in PIPL, being the collection, storage, use, processing, transmission, provision, disclosure, and deletion of Personal Information;
- 1.9 "Personal Information Processor" has the meaning of "personal information processor" as defined in PIPL, being the individual or organization who independently determines the purpose and mean of Processing of Personal Information; and

- 1.10 “Sensitive Personal Information” has the meaning of “special personal information” as defined in PIPL, being Personal Information once leaked or illegally used, will easily lead to infringement of the human dignity or harm to the personal or property safety of a natural person, including biometric recognition, religious belief, specific identity, medical and health, financial account, personal location tracking and other similar information of a natural person, as well as any Personal Information of a minor under the age of 14.

## 2. OBLIGATIONS OF THE DATA EXPORTER AND DATA IMPORTER

- 2.1 The Data Exporter and the Data Importer agree to comply with the provisions of PIPL in respect of any transfer and subsequent Processing of the Personal Information, as may be applicable.
- 2.2 The Data Exporter and Data Importer are required to comply with all the provisions and obligations as set out in the DPA, as read with the relevant provisions of PIPL. For the avoidance of doubt, this will include the provisions and obligations that make express reference to certain articles of the GDPR.
- 2.3 Except where separate consent is not required for cross-border transfer of Personal Information in accordance with PIPL, the Data Exporter shall obtain the required consent from the Data Subjects for transfer of Personal Information to the Data Importer and warranty that the consent obtained are in compliance with the requirements of PIPL.
- 2.4 If the Data Exporter is required to store the Personal Information in China under PIPL, the Data Exporter 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 the Data Importer shall return or destruct the Personal Information held by it at the choice of the Data Exporter without undue delay.
- 2.5 The Data Importer agrees to assist the Data Exporter in every proper way to comply with PIPL and satisfy requirements of the Competent Supervisory Authority, including (i) reporting to the Competent Supervisory Authority or notifying the relevant Data Subjects about a personal information breach, (ii) responding to Data Subjects' requests for the exercise of their rights under PIPL, (iii) signing the model clauses for cross-border transfer of personal information issued by the Competent Supervisory Authority, and (iv) providing information and access to the Data Exporter or its engaged consultants or professional service providers for implementation of personal information protection impact assessment or security assessment.
- 2.6 If there is change of control or substantial change of business scope of the Data Importer, or change in the laws of the location of storage of the Personal Information, which may cause threats to the security of Personal Information, the Data Importer shall take security measures reasonably requested by the Data Exporter to mitigate any such threats on the security of Personal Information.
- 2.7 The Data Importer shall only disclose the Personal Information to a third party located outside China (in the same country as the data importer or in another third country) if the third party is or agrees to be bound by this Schedule 5 and the DPA.
- 2.8 In complying with these obligations, the following terms in this Schedule 5 shall have the following meanings in the DPA:
- 2.8.1 “Personal Information” shall replace and substitute the term “personal data”;
- 2.8.2 “Sensitive Personal Information” shall replace and substitute the term “sensitive data” and the relevant categories of sensitive data listed in the “Sensitive Data” section of the DPA;
- 2.8.3 “Data Subject” shall have the meaning as set out in this Schedule 5;

- 2.8.4 "Personal Information Processor" shall replace and substitute the term "controller";
- 2.8.5 "Entrusted Party" shall replace and substitute the term "processor";
- 2.8.6 "Processing" or "Process" shall have the meaning as set out in this Schedule 5; and
- 2.8.7 "Competent Supervisory Authority" shall have the meaning as set out in this Schedule 5.

### **3. GOVERNING LAW AND JURISDICTION**

- 3.1 This Schedule 5 read together with the DPA shall be governed by and construed in accordance with the laws of the People's Republic of China ("PRC").
- 3.2 Any dispute arising from this Schedule 5 read together with the DPA shall be resolved by the courts in the PRC. The Parties agree to submit themselves to the jurisdiction of such courts.

## Schedule 6: Taiwan Data Processing Requirements

This annexure applies to Customers who are domiciled in Taiwan or who are not domiciled in Taiwan but make use of automatic or non-automatic means in Taiwan to process Personal Data. In terms of the Service Agreement, the Customer (as the Data Exporter) may be required to transfer Personal Data to WTG entities (as the Data Importer), which entities may be situated outside of Taiwan in order to, amongst other things, carry out the services in terms of the Service Agreement.

In order to ensure adequate safeguards for the cross-border transfer of the Personal Data in accordance with the provisions of the PDPA, the Parties agree that the Customer shall be entitled to transfer Personal Data to WTG, and WTG shall be entitled to receive and Process the Personal Data, subject to the terms and conditions set out in this Schedule 6 as read together with the DPA.

### DEFINITIONS

For the purposes of this Schedule 6, the following words will have the following meanings and cognate expressions shall have corresponding meanings:

- i. "Commissioned Agency" has the same meaning as "commissioned agency" as defined in the PDPA being a person or entity collecting, Processing, and/or using personal data under the commission or on behalf of others;
- ii. "Data Exporter" means the Customer who processes and transfers Personal Data to the Data Importer.
- iii. "Data Importer" means the applicable WTG entity, who receives Personal Data from the Data Exporter for Processing in accordance with the terms of this Schedule 6;
- iv. "Data Subject" has the same meaning as "data subject" as defined in the PDPA being a natural person whose Personal Data is collected, Processed or used;
- v. "Non-government Agency" has the same meaning as "non-government agency" as defined in the PDPA being any natural person, juristic person or unincorporated association which is not a government agency;
- vi. "PDPA" means the Taiwan Personal Data Protection Act, including any regulations, codes of conduct, directions, rulings or other interpretative instruments promulgated or made thereunder, as amended from time to time;
- vii. "Personal Data" has the meaning of "personal data" as defined in PDPA, being information relating to a natural person's name, date of birth, national ID card number, passport number, appearance features, fingerprints, marital status, family background, educational background, occupation, contact information, financial status, social activities, and any other data that may be used to directly or indirectly identify a natural person. For the avoidance of doubt, "Personal Data" shall include "Special Category Personal Data";
- viii. "Processing" or "Process" covers any operation or activity concerning Personal Data which falls within the meaning of "processing" or "use" as defined in the PDPA, including but not limited to, the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, retention, alteration, use, disclosure, access, transfer, distribution, linking, merging, degradation, erasure or destruction;
- ix. "Special Category Personal Data" refers to Personal Data concerning medical history, medical treatments, genealogy, sex life, health-check results, and criminal records.

## OBLIGATIONS OF THE DATA EXPORTER AND DATA IMPORTER

The Data Exporter and the Data Importer agree to comply with the provisions of the PDPA in respect of any transfer and subsequent Processing of the Personal Data, as may be applicable.

The Data Exporter and Data Importer are required to comply with all the provisions and obligations as set out in the DPA, as read with the relevant provisions of the PDPA. For the avoidance of doubt, this will include the provisions and obligations that make express reference to certain articles of the GDPR.

In complying with these obligations, the following terms in this Schedule 6 shall have the following meanings in the DPA:

- a. "Personal Data" shall replace and substitute the term "personal information";
- b. "Special Category Personal Data" shall replace and substitute the term "sensitive data";
- c. "Data subject" shall have the meaning as set out in this Schedule 6;
- d. "Non-government Agency" shall replace and substitute the term "controller"
- e. "Commissioned Agency" shall replace and substitute the term "processor"; and
- f. "Processing" or "Process" shall have the meaning as set out in this Schedule 6.

## GOVERNING LAW AND JURISDICTION

This Schedule 6 read together with the DPA shall be governed by and construed in accordance with the laws of the Republic of China (Taiwan).

Any dispute arising from this Schedule 6 read together with the DPA shall be resolved by the courts in Taiwan and the Parties agree to submit themselves to the jurisdiction of the Taiwan Taipei District Court.

## Schedule 7: South African Data Processing Requirements

This Schedule 7 applies to Customers who are domiciled in South Africa or who are not domiciled in South Africa but make use of automatic or non-automatic means in South Africa to process Personal Information. In terms of the Service Agreement, the Customer (as the Data Exporter) may be required to transfer Personal Information to WTG entities (as the Data Importer), which entities may be situated outside of South Africa in order to, amongst other things, carry out the services in terms of the Service Agreement.

In order to ensure adequate safeguards for the cross-border transfer of the Personal Information in accordance with the provisions of POPIA, the Parties agree that the Customer shall be entitled to transfer Personal Information to WTG, and WTG shall be entitled to receive and Process the Personal Information, subject to the terms and conditions set out in this Schedule 7 as read together with the DPA.

### 1. DEFINITIONS

For the purposes of this Schedule 7, the following words will have the following meanings and cognate expressions shall have corresponding meanings:

- 1.1 "Data Exporter" means the Customer who processes and transfers Personal Information to the Data Importer;
- 1.2 "Data Importer" means the applicable WTG entity, who receives Personal Information from the Data Exporter for processing in accordance with the terms of this Schedule 7 and who is not subject to laws ensuring adequate protection as contemplated in section 72 of POPIA;
- 1.3 "Data Subject" has the same meaning as "data subject" as defined in POPIA being a natural or juristic person to whom the Personal Information relates;
- 1.4 "Personal Information" has the meaning of "personal information" as defined in POPIA, being information relating to an identifiable, living, natural person, and where it is applicable, an identifiable existing juristic person, including but not limited to –
  - a. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
  - b. information relating to the education or the medical, financial, criminal or employment history of the person;
  - c. any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
  - d. the biometric information of the person;
  - e. the personal opinions, views or preferences of the person;
  - f. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
  - g. the views or opinions of another individual about the person; and
  - h. the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person; and
  - i. for the avoidance of doubt, "Personal Information" shall include "Special Personal Information";

- 1.5 “Operator” has the same meaning of “operator” as defined in POPIA, being a person who processes Personal Information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;
- 1.6 “POPIA” means the Protection of Personal Information Act 4 of 2013, including any Regulations, Codes of Conduct, Directions, Rulings or other interpretative instruments promulgated or made thereunder, as amended from time to time;
- 1.7 “Processing” or “Process” has the same meaning of “processing” as defined in POPIA being any operation or activity or any set of operations concerning Personal Information, including but not limited to, the collection, receipt, recording, organization, collation, storage, updating, or modification, retrieval, retention, alteration, use, disclosure, access, transfer, distribution, linking, merging, degradation, erasure or destruction;
- 1.8 “Responsible party” has the same meaning as “responsible party” as defined in POPIA being a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;
- 1.9 “Special Personal Information” has the same meaning as “special personal information” defined in POPIA being Personal Information concerning an individual’s: religious or philosophical beliefs, race or ethnic origin; trade union membership; political persuasion; health or sex life; biometric information; or criminal behaviour; and
- 1.10 “Supervising Authority” has the same meaning as “Regulator” as defined in POPIA, being the Information Regulator established in terms of section 39 of POPIA.

## **2. OBLIGATIONS OF THE DATA EXPORTER AND DATA IMPORTER**

- 2.1 The Data Exporter and the Data Importer agree to comply with the provisions of POPIA in respect of any transfer and subsequent Processing of the Personal Information, as may be applicable.
- 2.2 The Data Exporter and Data Importer are required to comply with all the provisions and obligations as set out in the DPA, as read with the relevant provisions of POPIA. For the avoidance of doubt, this will include the provisions and obligations that make express reference to certain articles of the GDPR.
- 2.3 In complying with these obligations, the following terms in this Schedule 7 shall have the following meanings in the DPA:
  - 2.3.1 “Personal Information” shall replace and substitute the term “personal data”;
  - 2.3.2 “Special Personal Information” shall replace and substitute the term “sensitive data”;
  - 2.3.3 “Data subject” shall have the meaning as set out in this Schedule 7;
  - 2.3.4 “Responsible party” shall replace and substitute the term “controller”;
  - 2.3.5 “Operator” shall replace and substitute the term “processor”;
  - 2.3.6 “Processing” or “Process” shall have the meaning as set out in this Schedule 7; and
  - 2.3.7 “Supervising Authority” shall have the meaning as set out in this Schedule 7.

## **3. GOVERNING LAW AND JURISDICTION**

- 3.1 This Schedule 7 read together with the DPA shall be governed by and construed in accordance with the laws of the Republic of South Africa.
- 3.2 Any dispute arising from this Schedule 7 read together with the DPA shall be resolved by the courts in South Africa and the parties agree to submit themselves to the jurisdiction of the High Court of South Africa.



## Schedule 8: Brazil Data Processing Requirements

This Schedule 8 applies to (i) Customers domiciled in Brazil, or (ii) whose Personal Information has been collected in Brazil or (iii) who are not domiciled in Brazil but make use of automatic or non-automatic means offered in Brazil to process Personal Information. In terms of the Service Agreement, the Customer (as the Data Exporter) may be required to transfer Personal Information to WTG entities (as the Data Importer), which entities may be situated outside of Brazil in order to, amongst other things, carry out the services in terms of the Service Agreement.

In order to ensure adequate safeguards for the cross-border transfer of the Personal Information in accordance with the provisions of Brazil's Lei Geral de Proteção de Dados (or LGPD), the Parties agree that the Customer shall be entitled to transfer Personal Information to WTG, and WTG shall be entitled to receive and Process the Personal Information, subject to the terms and conditions set out in this Schedule 8 as read together with the DPA.

### 1. DEFINITIONS

For the purposes of this Schedule 8, the following words will have the following meanings and cognate expressions shall have corresponding meanings:

- 1.1 "International Transfer of Personal Information": transfer of Personal Information to a foreign country required for the performance of the subject matter.
- 1.2 "Data Exporter" means the Customer who processes and transfers Personal Information to the Data Importer.
- 1.3 "Data Importer" means the applicable WTG entity that receives Personal Information from the Data Exporter for processing, in accordance with the terms of this Supplement 8, and that is not subject to laws that ensure appropriate protection as set out in the LGPD;
- 1.4 "Data Subject" has the same meaning as defined in the LGPD, being an individual to whom Personal Information or Sensitive Personal Information relates or under the international laws of data of a Legal Entity;;
- 1.5 "Personal Information" has the meaning of "personal data" as defined in the LGPD, being information relating to an identified or identifiable individual. "Personal Information" has the meaning of "personal information" as defined in LGPD, being information relating to an identifiable, living, natural person, and where it is applicable, an identifiable existing juristic person, including but not limited to:
  - a. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
  - b. information relating to the education or the medical, financial, criminal or employment history of the person;
  - c. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
  - d. the biometric information of the person;
  - e. the personal opinions, views or preferences of the person;
  - f. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
  - g. the views or opinions of another individual about the person; and
  - h. the name of the person if it appears with other personal information relating to the person or if the

disclosure of the name itself would reveal information about the person; and

- i. for the avoidance of doubt, "Personal Information" shall include "Special Personal Information";

- 1.6 "Sensitive Personal Information": shall mean personal data concerning as defined a LGPD including when related to an individual;
- 1.7 "Processing" or "to Process" has the same meaning as "processing" as defined in the LGPD, being any operation or activity or any set of operations relating to Personal Information including, without limitation, collecting, receiving, recording, organizing, grouping, storing, updating or modifying, retrieving, retaining, altering, using, disclosing, accessing, transferring, distributing, linking, merging, degrading, erasing, or destroying.

## **2. PURPOSE OF THE COLLECTION AND PROCESSING OF PERSONAL INFORMATION**

WTG collects Personal Information from third parties through its Customers and, possibly Sensitive Personal Information, in order to provide services requested, including conducting work on the customers database for maintenance. Such Personal Information or Sensitive Personal Information will be used with the objective of making the execution of its service contracts feasible.

## **3. PROTECTION OF PERSONAL INFORMATION**

WTG uses its best efforts to safeguard Personal Information and Sensitive Personal Information of third parties provided by Customers, in order to avoid risks to privacy, and to protect the Data Subject from unauthorized access to information about him/her, undertaking to implement physical, administrative and technical security measures required for the protection of Personal Information against theft, loss, alteration, destruction, unauthorized use, access, handling or damage.

## **4. SHARED USE OF PERSONAL INFORMATION**

In order to meet contractual purposes, it is possible that Personal Information and Sensitive Personal Information may be shared in the following cases: a) third parties who need to process the information to carry out the business relationship with WTG; b) subcontracting companies by WTG which need to process the data to carry out the business relationship; c) use of data processing and storage companies by WTG, including those located abroad; and d) if required by a competent authority or applicable law that establish an obligation to share.

## **5. INTERNATIONAL TRANSFER OF PERSONAL INFORMATION**

In accordance with the Service Agreement, the Customer may transfer Personal Information and Sensitive Personal Information internationally ("Data Exporter") to WTG abroad ("Data Importer") for: (a) the search and fulfillment of the purposes for which it was provided; (b) to comply with contractual and legal provisions; and (c) pursuant to a court order or request. If necessary, WTG will perform International Transfer of Personal Information to subcontractors for the fulfillment of contracts or, further, in case of requirement for the due fulfillment of its legal obligations, for the promotion of legitimate interest of WTG and in the other cases provided by the LGPD.

The Parties agree that the Customer shall transfer Personal Information to WTG, and WTG shall have the right to receive and Process the Personal Information (and Sensitive Personal Information, if applicable), subject to the terms and conditions set forth in this Schedule 8 and pursuant to the provisions of DPA.

## 6. OBLIGATIONS OF THE DATA EXPORTER AND IMPORTER

The Data Exporter and the Data Importer agree to comply with the provisions of the LGPD in relation to any International Information Transfer and subsequent Processing of the Personal Information, as applicable, and the Data Exporter shall be responsible for obtaining the consent of the Data Subject to the processing of the Personal Information and Sensitive Personal Information.

The Data Exporter and the Data Importer are required to comply with all other provisions and obligations set forth in the DPA, and pursuant to the provisions of the LGPD.

## 7. GOVERNING LAW AND JURISDICTION

This Schedule 8, combined with the DPA, shall be governed by and construed in accordance with the laws of Brazil.

Any dispute arising out of this Supplement 8 and in combination with the DPA shall be settled by the courts of Brazil and the Parties undertake to be subject to the jurisdiction of the Courts of Brazil.

## 8. DATA PROTECTION OFFICER

The Data Subject may exercise the rights by a written request via email to 'The Data Protection Officer for Brazil', for the purposes of this DPA and this Supplement 8, through the email addresses: carolina.michelini@wisetechglobal.com or luana.molina@wisetechglobal.com, and must inform (i) the name of the holder of the personal information; (ii) documents proving his/her identity; (iii) address to receive communications and response to his/her request; (iv) if he/she is a legal representative, the instrument from which the powers of representation come from; (v) provide clear and precise description of the personal information, in relation to which it is intended to exercise its rights; (vi) any other element that, according to the legislation and the latest Privacy Policy in force at the time of submission of the request.

## 9. FINAL PROVISIONS

WTG reserves the right to change or update this Schedule at any time, adjusting it due to compliance with applicable legislative changes or modifications deemed necessary or due to internal policies, for the provision or management of services or products.