Data Processing Agreement

INDEX

1. Preamble

1.1 This Data Processing Agreement is an Appendix of the Master Service Agreement between Nezasa AG, with offices at Sihlstrasse 99, 8001 Zurich, Switzerland (“Nezasa”) and the Customer. The Master Service Agreement has a set of Service Orders between Nezasa and the Customer attached (together with the Master Service Agreement the “Agreement”). The Customer and Nezasa form each a “Party” and together hereinafter referred to sometimes as the "Parties".

1.1. This Data Processing Agreement defines the responsibilities of the Parties in the area of data protection that arise from the Services provided under the Agreement. It is applied to all tasks in relation to the Agreement in which employees of Nezasa or persons contracted by Nezasa process personal data on behalf of Customer (in accordance with Art. 4 Nr. 8 and Art. 28 GDPR). For purposes of this Data Processing Agreement, Nezasa is a processor acting on behalf of the Customer. This Data Processing Agreement does not apply to Personal Data that Nezasa processes as a Controller.

1.2. This Data Processing Agreement defines the rights and duties of the Parties in relation to the processing of personal data and incorporates by reference, the appendices that appear at the end of the Agreement.

2. Subject Matter and Duration

2.1. The subject matter results from the Agreement.

2.2. The duration of the subject matter corresponds to the duration of the Agreement.

3. Specification of the Service Order(s) or Agreement Details

3.1. Nature and purpose of processing personal data by Nezasa for the Customer are precisely defined in the Agreement.

3.2. The undertaking of the contractually agreed data processing may be carried out partly outside of Switzerland, the EU or the EEA. The specific conditions of Art. 44 ff. GDPR is ensured as follows:

- Adequacy decision by the European Commission (Article 45 Paragraph 3 GDPR);
- Establishing Standard Data Protection Clauses, e.g. EU-Model Clauses (Article 46 Paragraph 2 Points c and d GDPR) as set out in Appendix C to this Data Processing Agreement;
- Established by other means (Article 46 Paragraph 2 Point a, Paragraph 3 Points a and b GDPR)

Nezasa shall enter into the EU-Model Clauses with Customers outside Switzerland, the EU and EEA where processing relates to EU citizens personal data. Upon request, Nezasa shall provide more detailed information on the measures taken.

Transfers to the UK: For the avoidance of doubt, when the European Union law ceases to apply to the United Kingdom ("UK") upon the UK's withdrawal from the European Union, and until such time as UK is deemed to provide adequate level of protection for Personal Data (within the meaning of applicable European Data Protection legislation), then to the extent Nezasa processes (or causes to be processed)

any Customer Data protected by European Data Protection legislation applicable to the EU/EEA and Switzerland in the UK, Nezasa shall process such Customer Data in compliance with the Standard Contractual Clauses Clauses or any applicable alternative transfer mechanism as described above.

3.3. Type of Data: The subject matter of the processing of personal data comprises the following data types/categories:

- User behaviour / navigation data
- Web browser information
- Audit data (e.g. who edited what when or logins)
- Contact data
- PAX data (contact data, date of birth, nationality, passport number, gender)
- Itinerary data (dates and schedule)
- Communication data (e.g. for contact requests)

3.4. Categories of Data Subjects: The Categories of data subjects comprise:

- Employees of the Customer
- Travel agents
- Travellers

4. Lawful Collection

4.1. Customer warrants towards Nezasa that any Personal Data disclosed to Nezasa was collected in a lawful manner and does not infringe upon the rights and freedoms of the Data Subject and/or third parties.

5. Technical and Organisational Measures

5.1. Nezasa has documented its Technical and Organisational Measures, set out in Appendix A to this Data Processing Agreement. Upon execution of this Data Processing Agreement (as an integral part of the Master Service Agreement), the documented measures become the foundation of the contract.

5.2. Nezasa shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account (Details in the Appendix to this Data Processing Agreement).

5.3. The Technical and Organisational Measures are subject to technical progress and further development. In this respect, Nezasa may implement adequate alternative measures. In so doing, the security level of the denied measures shall not be less than currently applied. Substantial changes shall be documented.

6. Rectification, Restriction and Erasure of Data

6.1 Nezasa may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Customer, but only on documented instructions from the Customer. Insofar as Data Subjects contact Nezasa directly concerning a rectification, erasure, or restriction of processing, Nezasa will immediately forward the Data Subject's request to the Customer.

6.2. Only insofar as it is included in the scope of Services, the erasure policy, 'right to be forgotten', rectication, data portability and access shall be ensured by Nezasa in accordance with documented instructions from the Customer without undue delay.

7. Quality Assurance and Other Duties of Nezasa

7.1. Nezasa shall comply with the following requirements:

a. Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. Nezasa entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. Nezasa and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from Customer, which includes the powers granted in this contract, unless required to do so by law.
b. Implementation of and compliance with all Technical and Organisational Measures necessary for the applicable Service Order(s) or Agreement in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR (details in Appendix A to the Data Processing Agreement).
c. Customer and Nezasa shall cooperate, on request, with the supervisory authority of Customer in performance of its tasks.
d. Customer shall be informed immediately of any inspections and measures conducted by the supervisory authority of Customer, insofar as they relate to the applicable Service Order(s) or Agreement. This also applies insofar as Nezasa is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of the applicable Service Order(s) or Agreement.
e. Insofar as the Customer is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the applicable Service Order(s) or Agreement, Nezasa shall use reasonable endeavours to support the Customer.
f. Nezasa shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within its area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

8. Subcontracting

8.1. Subcontracting for the purpose of this Data Processing Agreement is to be understood as meaning services which relate directly to the provision of the principal services. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. Nezasa shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of Customer's data, even in the case of outsourced ancillary services.

8.2. Nezasa may commission subcontractors (additional contract processors) at its own discretion in order to process personal data for the purposes set out in this Data Processing Agreement subject to the following conditions:

a. Nezasa imposes data protection terms on any appointed subcontractor that require such subcontractor to protect the personal data to the standard required by applicable data protection law;
b. Nezasa remains liable for any breach of this Data Processing Agreement caused by an act, error or omission of the appointed subcontractor; and
c. Nezasa provides the Customer with its then current list of any appointed subcontractor upon Customer’s request.

8.3. If the subcontractor provides the agreed service outside Switzerland or the EU/EEA, Nezasa shall ensure compliance with EU Data Protection Regulations by appropriate measures.

9. Supervisory Powers of Customer

9.1. Customer has the right, after consultation with Nezasa, to carry out inspections or to have them carried out by an auditor to be designated in each individual case at Customer’s own cost. It has the right to convince itself of the compliance with this Data Processing Agreement by Nezasa in its business operations by means of random checks, which must be announced well in advance and cause minimal disruption to business.

9.2. Nezasa shall ensure that the Customer is able to verify compliance with the obligations of Nezasa in accordance with Article 28 GDPR. Nezasa undertakes to give the Customer the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organisational Measures.

10. Communication in the Case of Infringements by Nezasa

10.1. Nezasa shall assist the Customer in complying with Customer's obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 GDPR. These include:

a. Ensuring an appropriate level of protection through Technical and Organisational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable immediate detection of relevant infringement events;
b. The obligation to report a personal data breach without undue delay to the Customer is subject to Article 33(2) GDPR;
c. The duty to assist the Customer with regard to the Customer's obligation to provide information to the Data Subject concerned and without undue delay, provide the Customer with all relevant information in this regard;
d. Supporting the Customer with its data protection impact assessment if requested; and
e. Supporting the Customer with regard to prior consultation of the supervisory authority.

10.2. Nezasa may claim compensation for support services which are not included in the description of the services but limited to which are not attributable to failures on the part of Nezasa.

11. Authority of Customer to issue instructions

11.1. Customers shall immediately confirm oral instructions regarding the data processing (at the minimum in text form).

11.2. Nezasa shall inform the Customer immediately if it considers that an instruction violates data protection regulations. Nezasa shall then be entitled to suspend the execution of the relevant instructions until the Customer confirms or changes them.

12. Liability

12.1. The provisions on liability of the Master Service Agreement apply.

13. Deletion and Return of Personal Data

13.1. Copies or duplicates of the Personal Data shall never be created without the knowledge of the Customer, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

13.2. After conclusion of the contracted work, or earlier upon request by the Customer, at the latest upon termination of the last Service Order between the Parties, subject to regulatory requirements Nezasa shall, on Customer request, hand over to the Customer or destroy all Personal Data sets related to the Agreement that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected tests, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

13.3. Documentation which is used to demonstrate orderly data processing in accordance with the applicable Service Order(s) or Agreement shall be stored beyond the contract duration by Nezasa in accordance with the respective retention periods. It may hand such documentation over to the

Customer at the end of the contract duration to relieve Nezasa of this contractual obligation.

Appendix A: Technical and Organisational Measures

A. Confidentiality (Art. 32 Abs. 1 lit. b GDPR)

CONTROL	IMPLEMENTED MEASURES
a) General / Data protection management Organizational Control	• All employees at the various sites receive security awareness training. • Different policies exist which define rules for data classification or information security. • mobile device management (MDM) was introduced company-wide for central administration and control
b) Physical Access Control No unauthorised access to Data Processing Facilities	**Nezasa Office Zurich**: • The Zurich office is located in a building whose main entry door is secured with a secret code. • The office rooms are separated from the stairway with a locked door. • The door to the office is secured with a Smart Lock (NUKI 2.0), which can only be activated through an app on the employee's phone after having been invited as a user. • This is done for all employees upon the start of their tenure and their access is removed on their last day. • Employees from other offices of Nezasa may be given temporary access for the duration of their stay. • To gain access to the premises, visitors need to ring the bell at the main entry door and are received at the office door by an employee of Nezasa. • The entrance door to Nezasa offices is secured with a safety lock. When locked, the door is additionally secured with security bolts in the ceiling, floor and laterally in the walls. **Nezasa Office Lisbon:** • The Lisbon office building has a 24/7 concierge to whom people who enter have to identify themselves. • The door to the office is secured with a Smart Lock (NUKI 2.0), which can only be activated through an app on the employee's phone after having been invited as a

	user. ● This is done for all employees upon the start of their tenure and their access is removed on their last day. ● Employees from other offices of Nezasa may be given temporary access for the duration of their stay. ● Visitors register with Nezasa and are received at the entrance of the building by a Nezasa employee.
c) Electronic Access Control No unauthorised use of the Data Processing and Data Storage Systems	● Access to workstations and notebooks is protected via individual user accounts. ● Access to servers is protected via separate administrator accounts. ● The circle of authorised persons is limited to the operationally necessary extent. ● 2-factor authentication using an authenticator App is enforced for critical systems that handle personal identifying data. ● Nezasa has an authorization concept that is documented in written form. ● Employees have personal accounts that can be revoked at any time. ● Nezasa uses a password manager for employees to generate passwords according to predefined password rules. Password rules include a minimum of 12 digits with at least one special character and upper and lower case letters.
d) Internal Access Control Permissions for user rights of access to and amendment of data. No unauthorised Reading, Copying, Changes or Deletion of Data within the system, e.g. rights authorisation concept, need-based rights of access, logging of system access events	● Access authorizations are assigned in the applications on a role-based basis. The principle of "need-to-know" and "need-to-do" is applied. ● Role-based distinction is made between write, read and delete authorizations. ● Each authorised user can only access data that he or she needs to perform the assigned tasks and functions. ● Binding written regulations exist for handling access data. ● There are no local deployments of sensitive Customer Data. ● Nezasa has an authorization concept that is documented in written form.

	• All Nezasa-internal software implements the authorization concept. • Employees have personal accounts that can be revoked at any time. • The number of system administrators is reduced to the minimum (only engineering management). • When an employee leaves Nezasa, it is ensured that all accounts and permissions are revoked immediately (with a checklist). • Nezasa does not store personal data on paper.
e) Isolation Control Isolated Processing of Data, which is collected for differing purposes	• Separation of production, test and development systems with separate application instances and databases. • Dedicated permissions for the production system. • Logical isolation of data by implementation of a multi-tenancy concept. • Accessing data of other tenants is prevented by the system.
f) Pseudonymisation (Art. 32 Abs. 1 lit. a GDPR; Art. 25 Abs. 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.	• On testing & development systems, Customer Data is pseudonymized.

B. Integrity (Art. 32 Abs. 1 lit. b GDPR)

CONTROL	IMPLEMENTED MEASURES

a) Data Transfer Control No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport	• Communication between the System of Nezasa, the Customer and third parties is encrypted (HTTPS). • Nezasa maintains a data retention policy. • All data storage on Nezasa computers is encrypted. • Paper is destroyed according to DIN/EN/ISO 66399 security level P-4 with a shredder in the office.

b) Data Entry Control
 	
Verification, whether and by whom Personal Data is entered into a Data Processing System, is changed or deleted
	• The objects contain the following attributes that must be updated with each change:
	  · Author
	  · Creation timestamp
	  · Author of the modification
	  · Modification timestamp
	• The technical attributes can be read from the database by Nezasa.
	• The most current value of the attributes can be visible in the backup application (e.g. last modified).
	• Automated, daily backups are created for all data to enforce traceability.

C. Availability and Resilience (Art. 32 Abs. 1 lit. b GDPR)

CONTROL	IMPLEMENTED MEASURES
a) Availability Control Prevention of accidental or wilful destruction or loss; Rapid Recovery (Art. 32 Abs. 1 lit. c GDPR)	• The data centre of the service provider Amazon AWS in Dublin (Ireland) has been certified according to ISO 27001, ISO 27017 and ISO 27018. • The system has been set up as a distributed system and can be scaled in case of a high load at any time. The database architecture is based on a master/slave setup. The application uses multiple instances which can replace each other at any time. • For more details see AWS TOM.

	• Backups of the data stored on AWS are carried out daily and stored on a secondary cloud provider according to an internal retention policy.

D. Procedures for Regular Testing, Assessment and Evaluation (Art. 32 Abs. 1 lit. d GDPR; Art. 25 Abs. 1 GDPR)

CONTROL	IMPLEMENTED MEASURES
a) Data Protection Management	• Data protection is a regular agenda item at management meetings. The corresponding discussions and decisions are logged in a data protection log. • The employees of Nezasa are informed about the applicable data protection procedures and guidelines at entry and are informed about the corresponding duties in written form.
b) Contract Supervision	• All employees handling personal data have committed themselves to confidentiality. • Processing solely under and according to data processing agreement and subject to directives from our customers

Appendix B: Data Processing Appendix

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data Exporter: The data exporter is: Nezasa AG, (Nezasa AG, Sihlstrasse 99, CH-8001 Zurich, Switzerland), under a mandate from Customer

Data Importer: The data importer is: Customer

Nature of Services: The Nature of Services are set out in the Agreement which describes the provision of services to the Customer.

Categories of Data Subjects: These are set out in clauses 3.3 and 3.4 of the Agreement.

Categories of Data Processed: The personal data processed concerns the following categories of data: Any Customer Data processed by Nezasa in connection with the Services and which could constitute any type of personal data or personal information.

Special Categories of Data (if applicable): n/a

Processing Operations: The personal data processed will be subject to the following basic processing activities (please specify):

- Personal Data will be transferred from the Customer to Platform for purposes of planning and booking of individual travels including supporting and processing services provided by third parties.

Appendix C: 2021 Standard Contractual Clauses for the Transfer of Personal Data From the Community to Third Countries (Controller to Processor transfers)

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) ([1]) for the transfer of 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

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

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.

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 ([2]) (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,

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of 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 thirty calendar 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. ([3]) 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.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([4]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(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:

(i) 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;

(ii) 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.

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(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) 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 ([5]);

(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.

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(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 Austria.

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 Austria.

(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.

ANNEX I

A. LIST OF PARTIES

See Appendix B of the Data Processing Agreement.

B. DESCRIPTION OF TRANSFER

See Appendix B of the Data Processing Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

See Clause 13 of these Standard Contractual Clauses..

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

The Technical and Organisational Measures are described in Appendix A of the Data Processing Agreement.

ANNEX III: LIST OF SUB-PROCESSORS

The List of Subprocessors will be provided to the Customer at any time upon request.

Previous Versions

Below are listed the previous versions of our Data Processing Agreement with the dates that they were published.

Version Oct 31st 2022: Part of https://nezasa.com/customer-terms-of-service-october-2022/