



## CUSTOMER TERMS OF SERVICE OF NEZASA AG

Our Customer Terms of Service is an agreement between Nezasa AG, with offices at Sihlstrasse 99, 8001 Zurich, Switzerland (“Nezasa”) and the Customer. The Customer and Nezasa form each a “Party” and together hereinafter referred to sometimes as the "Parties". Any capitalized terms used in these Service Terms shall have the meanings set forth in the Annex (Definitions) of the Master Service Agreement.

Nezasa’s Customer Terms of Service consists of the following terms:

**1. Terms for Support Services (Support SLA)**

Terms that apply to the Support Services included with our Subscription Services.

**2. Terms for Platform (Platform SLA)**

Terms that apply to the Customer’s use of our Platform, its services as well as third party services. This includes the Platform SLA.

**3. Terms for System Setup**

Terms that define the scope of the initial setup of the Platform Services and Support Services (together make the Subscription Services).

**4. Terms for Premium Services**

Terms that apply to the optional Premium Services in the form of Premium Platform Services and Premium Professional Services.

**5. Terms for Third Party Services**

Terms that apply to the use of Third Party Services that are used within the context of the Services provided.

**6. Data Processing Agreement (DPA)**

Terms that regard how we collect, receive, use, store, share, transfer, and process your personal data in connection with your use of the Subscription Services and Premium Services that together form the Services.

## **1. Terms for Support Services (Support SLA)**

The following terms relate to the Support Services included in Nezasa's Subscription Services and constitutes the Support SLA.

### **1.1 Support Services Description**

The scope of the Support Services is defined as following:

#### **Included (in scope):**

- User support related to use and parameterisation of the Platform.
- Technical support of the Platform.
- Technical support related to the Nezasa APIs.
- Support on billing of Platform-related matters.
- Dispatching of issues related to third party services towards the respective party.
- Access to the Nezasa knowledge base including standardized onboarding, tutorials and training sessions.

#### **Excluded (out-of-scope):**

- End users (travelers) support regarding planning, booking and post booking issues.
- Parametrization of product inventory.
- Support on booking and post booking handling with custom suppliers.
- Support for any software that is not part of the platform which also includes issues resulting from use of the APIs that do not relate to the API itself.
- Support of interfaces of the Customer that are not part of the Platform.
- Support of any hardware or other associated equipment of the Customer which is necessary to use the Platform or which are connected therewith.
- Custom elements and modifications of the code.
- Third party integrations not listed in-app as being supported by Nezasa.
- Any changes of code such as custom development service.
- Support of issues related to custom supply and services provided by third parties.
- Individual customised training sessions.

Support requests (the "Requests") pertaining to matters not explicitly stated in the above shall per default be considered excluded (out-of scope). Such Requests would only be addressed as a Premium Professional Service and be governed by the respective terms.

### **1.2 Support Services Availability**

Support Services Availability is dependent on the Support Plan agreed upon in the respective Service Order. The Support Plans are defined as follows:

Support Plan	Self-Service	Standard	Premium	24/7
Support Hours	Mon - Fri 09:00-17:00	Mon - Fri 09:00-17:00	Mon - Fri 09:00-20:00 Sat 08:00-16:00	7x24h
Meaningful First Response Time (during support hours)	Best endeavors	8 hrs High Priority: 4 hrs	4 hours High Priority: 2 hrs	4 hours High Priority: 60 min
Support Languages	EN	EN	EN ES during Support Hours	EN ES during Support Hours
Support via Support Hub	Yes	Yes	Yes	Yes
Support via Email	No	Yes	Yes	Yes
In-App Support	No	No	Yes	Yes
Emergency Telephone Contact Number	No	No	Yes	Yes
Emergency Telephone Support Hours	No	No	7x24h	7x24h
Emergency Telephone Response Time	No	No	60 min	60 min

**Support Hours:** The days and times during which the Nezasa customer service is accessible. For the service hours indicated, Zurich (Switzerland) timezone (CET) and business days are applicable.

**Meaningful First Response Time:** The time period within which Nezasa shall deliver a response to a Customer confirming that Nezasa received a Request and has commenced working on the issue. Nezasa attempts to respond according to the Support Plan’s specific response time. Outside of business days and hours, the response time is suspended except for emergency requests as described below. To better understand what Nezasa classifies as a High Priority Request read:

<https://support.nezasa.com/hc/en-gb/articles/13831583264145-Support-Tickets-Assessment>

**Emergency Request:** A Request that is solely reserved for critical issues which have a major impact on the Customer’s business. Such cases must be severe in nature, meaning that a large number of users or critical functions are affected and business processes are not possible or substantially impeded. To better understand what Nezasa classifies as a Emergency Request read:

<https://support.nezasa.com/hc/en-gb/articles/13831583264145-Support-Tickets-Assessment>

**Emergency Contact:** A Nezasa employee that is designated to answer Emergency Requests. Customers with a contractually agreed Support Plan containing an emergency contact receive an emergency email address and phone number. This contact information must be kept confidential and only be used in case of an emergency request. Improper use of the service may result in additional charges or a temporary suspension of the available service.

**Emergency Telephone Support Hours:** The days and times during which the emergency contact is accessible for emergency requests.

**Emergency Telephone Response Time:** The time period within which the emergency contact shall deliver a response to a Customer confirming that Nezasa received the emergency request and has commenced working on the issue. Nezasa attempts to respond according to the Support Plan specific response time.

**Support Language:** The languages in which Nezasa is able to provide customer support when answering to Requests. To avoid misunderstandings and delays in responding to Requests, Customers need to use one of the contractually agreed support languages. Deviations will likely result in delays which are not considered an infringement of the Support SLA provided.

**Support via Email:** Customer support provided through email. In order to contact Nezasa, Customers are asked to write an email to [support@nezasa.com](mailto:support@nezasa.com). Deviations will likely result in delays which are not considered an infringement of the Support SLA provided.

**Support via Phone:** Customer support provided by phone. Customers with a contractually agreed Support Plan that covers phone assistance in addition to email and in-app support can contact the provided phone number.

**In-App Support:** Nezasa offers in-app support on its Platform in the form of direct access to relevant knowledge base articles. New services such as live chat based on business hours may be introduced.

**Support via Support Hub:** Customer support provided via Nezasa's Support Hub through the "Submit a request" support form. Nezasa offers around the clock access to its self-service Support Hub on <https://support.nezasa.com> providing how-to articles, tutorials, video training as well as developer documentation. Deviations will likely result in delays which are not considered an infringement of the Support SLA provided.

**Denial of Service:** We may limit or deny your access to Support Services if we determine, in our reasonable discretion, that you are acting, or have acted, in a way that results or has resulted in misuse of support or abuse of Nezasa representatives and/or Services.

## 2. Terms for the Platform Services

The following terms relate to the Platform and its services. They can be changed or updated by Nezasa on its sole discretion at any time, to ensure the ever-evolving nature of the Platform is reflected appropriately.

## 2.1 Platform Services Description

Platform consists of various platform elements (the “Elements”). Which Elements are included in the Customer’s subscription must be defined in a Service Order. Elements that are not yet covered in a Service Order may be requested by the Customer at an additional cost.

### TripBuilder

Each element has a standard functionality described under the following link that is always available if the corresponding element has been subscribed to by the Customer plus potential Add-Ons that may be subject to additional fees:

<https://support.nezasa.com/hc/articles/4402965103889-What-is-TripBuilder->

The following Elements are available:

#### Application Modules:

- Cockpit - Customer Care
- Cockpit - Template Management
- Cockpit - Product Management
- Cockpit - Standard Settings
- Cockpit - Distribution Channel Settings
- Cockpit - User and Agency Management
- Discovery
- Planner
- Checkout
- Travel Documentation Generator

#### Connectors

- Supply Connectors
- Payment Connectors
- CRS Connectors
- Mid- and Back Office Connectors

For full list of adapters see:

<https://support.nezasa.com/hc/articles/4402965103889-What-is-TripBuilder->

#### APIs:

- Discovery API
- Itinerary API
- Planner API
- Booking API
- Location API
- Booking API Webhooks
- Inventory API

#### Deployment Options:

- Distribution Channels

**TripOptimizer**

Each element has a standard functionality described under the following link that is always available if the corresponding element has been subscribed to by the Customer plus potential Add-Ons that may be subject to additional fees:

<https://support.nezasa.com/hc/en-gb/articles/10038327738641-What-is-TripOptimizer->

The following Elements are available:

**Application Modules:**

- TripOptimizer - Airports/City Search
- TripOptimizer - Atomic Search
- TripOptimizer - One Destination Search
- TripOptimizer - Multi Destination Search
- Backoffice - Agency Management
- Backoffice - User Management
- Backoffice - Plans Management
- Backoffice - Providers Management

**Connectors:**

- GDS Connectors

**APIs:**

- SaaS API

**2.2 Platform Services Availability (Platform SLA)**

Nezasa uses a high availability infrastructure setup as well as additional commercially reasonable efforts that the Platform will be available by at least one of different access means to the Customer 24 hours per day, 7 days a week. We do target the following monthly availability percentage:

Product Plan	Optimize Standard	Optimize Premium	Monetize Standard	Monetize Premium	Maximize Standard	Maximize Premium
Availability Percentage	98.0%	98.5%	98.5%	99.0%	99.2%	99.5%

**Monthly Availability:** The total number of minutes in a calendar month minus the number of minutes of unavailability suffered in a calendar month, divided by the total number of minutes in a calendar month.

**Monthly Unavailability:** The time in which the Platform is not available as monitored out of an American and/or European region of a major cloud provider, excluding the time for scheduled and emergency maintenance.

Example: An Platform SLA of 99.5% means that the unavailability in a specific calendar month should not exceed cumulative time of 3 hours and 40 minutes.

**Scheduled Maintenance:** The scheduled downtime of the Platform required for maintenance purposes. Scheduled maintenance is excluded from the monthly downtime calculation up to a maximum of 144 hours per calendar year. Nezasa shall communicate scheduled maintenance to the Customer in writing at least 5 business days ahead of time.

**Emergency Maintenance:** The Platform maintenance that is not scheduled. For reasons beyond its reasonable control, Nezasa reserves the right to process emergency maintenance for which the normal notification time frame does not apply and a reason does not need to be communicated.

**Third Party Services Availability:** Third party product suppliers and other third party services which are connected to the Platform are excluded from the monthly downtime calculation. Nezasa is neither responsible nor liable for the availability of third party product suppliers and other third party services. Additional details of the third party services that can be used with TripBuilder and TripOptimizer and their commercial implications can be found on

<https://support.nezasa.com/hc/en-gb/articles/4402965074705-Third-Party-Services-Supplier-Products->

### 2.3 Connections to Supplier Products

The Platform allows Customers to connect to different external sources of travel products suppliers and services. It utilizes methods such as inventory management and data imports to draw upon content. It sends requests for price and availability data that unpins a live search functionality to build comprehensive itineraries for both Customers and end consumers. These itineraries are then bookable, changeable, and cancellable depending on the supplier's capabilities. These itineraries have automatic updating capabilities to reflect changes to the previously agreed services based on the supplier's technical capabilities and policies.

Third party suppliers may suspend, revoke or alter their services at any time and without any prior notice, depending on their service terms. Nezasa is therefore neither responsible nor liable for the content, its availability on the system landscape or the general availability of services provided by third party suppliers.

### 2.4 Acceptable Use Policy for the Platform

Nezasa reserves the right to limit, suspend, or stop providing parts or all of its Services if Customers use the Services in a way that causes legal liability to Nezasa or disrupts others' use of the Services or if the Customer's use of the Services is contrary to Nezasa's Acceptable Use Policy as outlined in these terms.

Any such violation may result in the loss of the Customer's rights to claim compensation under the Platform SLA or any other means stipulated in the Master Service Agreement.

The Acceptable Use Policy determines behaviour that Nezasa considers abusive that will lead to the suspension of Services:

**Disruption:**

- Compromising the integrity of our systems. This could include probing, scanning, or testing the vulnerability of any system or network that hosts our Services. This prohibition does not apply to security assessments expressly permitted by Nezasa.
- Tampering with, reverse-engineering, or hacking our Services, circumventing any security or authentication measures, or attempting to gain unauthorized access to the Services, related systems, networks, or data.
- Modifying, disabling, or compromising the integrity or performance of the Services or related systems, network or data.
- Deciphering any transmissions to or from the servers running the Services.
- Overwhelming or attempting to overwhelm our infrastructure by imposing an unreasonably large load on our systems that consume extraordinary resources (CPUs, memory, disk space, bandwidth, etc.), such as:
  - Using "robots," "spiders," "offline readers," or other automated systems to send more Requests to our servers than a human could reasonably send in the same period of time by using a normal browser.
  - Going far beyond the use parameters for any given Service as described in its corresponding documentation.
  - Performing actions that are inconsistent with and unrelated to the purposes for which the Services were designed.

**Wrongful activities:**

- Misrepresentation of yourself, or disguising the origin of any content (including by "spoofing", "phishing", manipulating headers or other identifiers, impersonating anyone else, or falsely implying any sponsorship or association with Nezasa or any third party).
- Using the Services to violate the privacy of others, including publishing or posting other people's private and confidential information without their express permission, or collecting or gathering other people's personal information (including account names or information) from our Services.
- Using our Services to stalk, harass, or post direct, specific threats of violence against others.
- Using the Services for any illegal purpose, or in violation of any laws (including without limitation data, privacy, and export control laws).
- Accessing or searching any part of the Services by any means other than our publicly supported interfaces (for example, "scraping").
- Using meta tags or any other "hidden text", including Nezasa's or our suppliers' product names or trademarks.



- Using the Services for the purpose of providing alerts on disaster scenarios or any other situations directly related to health or safety, including but not limited to acts of terrorism, natural disasters, or emergency response.

**Inappropriate communications:**

- Using the Services to generate or send unsolicited communications, advertising, chain letters, or spam.
- Soliciting our users for commercial purposes, unless expressly permitted by Nezasa.
- Disparaging Nezasa or our partners, vendors, or affiliates.
- Promoting or advertising products or Services other than your own without appropriate authorization.

**Inappropriate content:**

Posting, uploading, sharing, submitting, or otherwise providing content that:

- Infringes Nezasa’s or a third party’s intellectual property or other rights, including any copyright, trademark, patent, trade secret, moral rights, privacy rights of publicity, or any other intellectual property right or proprietary or contractual right.
- You don’t have the right to submit.
- Is deceptive, fraudulent, illegal, obscene, defamatory, libellous, threatening, harmful to minors, pornographic (including child pornography, which we will remove and report to law enforcement, including the National Center for Missing and Exploited Children), indecent, harassing, hateful.
- Encourages illegal or tortious conduct that is otherwise inappropriate.
- Attacks others based on their race, ethnicity, national origin, religion, sex, gender, sexual orientation, disability, or medical condition.
- Contains viruses, bots, worms, scripting exploits, or other similar materials.
- Is intended to be inflammatory.
- Could otherwise cause damage to Nezasa or any third party.

In this Acceptable Use Policy, the term “content” means: (1) any information, data, text, software, code, scripts, music, sound, photos, graphics, videos, messages, tags, interactive features, or other materials that you post, upload, share, submit, or otherwise provide in any manner to the Services and (2) any other materials, content, or data you provide to Nezasa or use with the Services.

### **3. Terms for System Setup**

#### **3.1 New System Setup**

##### **TripBuilder**

Unless agreed differently in a Service Order, the following terms relate to the setup of Nezasa’s TripBuilder for new Customers. They can be changed or updated by Nezasa at its sole discretion at any time.

**Included:**

- SaaS setup of a customer-specific TripBuilder based on the latest product version.
- Initial configuration of the instance as well as one distribution channel.
- Initial configuration of product supply with marketplace credentials.
- Initial configuration of languages, currencies and FX rates.
- White-Labeling: Brand Name, Logo & Basic Theming according to customer's corporate identity/design definition.
- Destination content from Nezasa covering major destinations.
- Hotel mappings from GIATA MultiCodes (MC).
- Hotel non-bookable content (NBC) from GIATA and MHG.
- Initial configuration of admin users.
- Initial configuration of product supply with custom credentials, for applicable Product Plans only.
- Up to 4 hours of training.

**Excluded (out-of-scope):**

- Any custom development.
- Parametrization of product inventory.
- Direct cost of third party services (e.g. for setup, operations, activation, certification, etc.).
- Necessary contracts of Customers with consolidators, travel product suppliers, mid/back-office suppliers and/or payment service providers.
- Necessary API key from Customer for the use of Google Maps.
- Necessary API key from Customer for the use of GIATA in case hotel information is shown in a customer-specific UI or in case the Customer intends to use Expedia supply with its own Expedia contract.
- Advanced theming exceeds via UI configurable elements.
- Custom labels and messages.
- Custom import jobs.

**TripOptimizer**

Unless agreed differently in a Service Order, the following terms relate to the setup of Nezasa's TripOptimizer for new Customers. They can be changed or updated by Nezasa at its sole discretion at any time.

**Included:**

- Initial Configuration of Agency
- Initial configuration of languages and currencies.
- Basic supplier configuration
- White-Labeling: Brand Name, Logo & Customer URL with Subdomain according to customer's corporate identity/design definition, if applicable to Product Plan.
- Advanced providers configuration such as provider credentials, booking activation, queue name for PNR, for applicable Product Plans only.

- Advanced provider configuration options, such as provider credentials, booking activation, and queue name for PNR, are available only for applicable product plans. Configuration options are based on provider and on Office ID/PCC.
- Initial configuration of users and admin users.

**Excluded (out-of-scope)**

- Any custom development.
- Parametrization of product inventory.
- Direct cost of third party services (e.g. for setup, operations, activation, certification, etc.).
- Necessary contracts of Customers with consolidators, travel product suppliers and payment service providers.
- Advanced theming exceeds via UI configurable elements.
- Custom labels and messages.
- Custom import jobs.

Additional setup work pertaining to matters not explicitly stated in the above, or in excess of the amounts provided shall per default be considered excluded (out-of-scope). Such work would only be addressed as a Premium Professional Service and be governed by the respective terms.

**3.2 Changes on Existing System Components**

**TripBuilder**

Cases of upgrades or downgrades, which implicate changes to an existing TripBuilder setup are not covered by the terms for setups. Changes to the setup of an existing system follow the delivery principles below:

**Included:**

- Initial configuration of the specified add-on.
- Necessary adjustments of Platform configuration in case of upgrade or downgrades.
- Necessary adjustments of the product supply configuration.
- Basic theming (set logo, font, colours) according to Customer’s corporate identity/design definition.

**Excluded (out-of-scope):**

- Any custom development service.
- Parametrization which the Customer can do via back office admin interface.
- Direct cost of third party services.
- Advanced theming exceeds via UI configurable elements.
- Custom labels and messages.
- Custom import jobs.

**TripOptimizer**

Cases of upgrades or downgrades, which implicate changes to an existing TripOptimizer setup are not covered by the terms for setups. Changes to the setup of an existing system follow the delivery principles below:

**Included:**

- Initial configuration of the specified add-on.
- Necessary adjustments of Platform configuration in case of upgrades or downgrades.
- Necessary adjustments of the product supply configuration.
- White-Labeling (set logo) according to Customer's corporate identity/design definition.

**Excluded (out-of-scope):**

- Any custom development service.
- Parametrization which the Customer can do via back office admin interface.
- Direct cost of third party services.
- Advanced theming exceeds via UI configurable elements.
- Custom labels and messages.
- Custom import jobs.

#### **4. Terms for Premium Services**

Premium Services refers to those additional services in Nezasa's portfolio that are not covered by the agreed service scope and Fees of the Subscription Services. Premium Services consist of two distinct offerings, Premium Professional Services and Premium Platform Services. Nezasa offers Premium Services on a discretionary basis to accommodate the needs of its Maximize Standard and Premium Customers who may require such services to realize the full potential of their solution.

**Premium Professional Services:** Are one-off knowledge-based services such as advisory, project management, and user training.

**Premium Platform Services:** An offering related to elements that directly impact the overall software driven capabilities of our Platform Services. These Premium Platform Services are a combination of one-time efforts and ongoing operations and maintenance work.

All Premium Services are dynamic in nature and Nezasa reserves the right to change their scope on an ongoing basis. All Premium Services are subject to a Service Order agreed between both parties.

##### **4.1. Premium Professional Services**

The following type of services are available as Professional Services:

**Advisory:** Nezasa provides, upon the request of a Customer, advice, an opinion or a plan in accordance with the Customer's request.

**Project Management:** Includes services such as the development of project plans and schedules, coordination and scheduling of project activities across stakeholders, facilitating project status meetings and reporting, managing project scope and deliverable requirements. If project management has been

agreed between the parties, it shall be authorised to act on behalf of the respective employees concerning all matters relating to the Premium Professional Services agreed.

**User Training:** Services related to the development of training material and courses for users of the Platform Services. Such user training may consist of remote and on-site courses, webinars, self-study material or other forms of written documentation.

**Delivery Mechanism & Timeline:** An Agreed Start Date is jointly established by both parties and captured in the relevant Service Order.

**Services Fee:** The fee to research, prepare and deliver a Premium Professional Service.

## 4.2. Premium Platform Services

### 4.2.1. Custom Platform Services (CPS)

**Custom Platform Services:** A combination of services including customer-specific software development delivered by Nezasa to address a particular business need and the ongoing support, operations and maintenance of this software service. This software capability is deemed by Nezasa to have no wider business relevance and is hence solely developed and operated for a particular Customer.

**Scoping:** The scope of a particular CPS is jointly agreed by both parties and captured in the relevant Service Order.

**Delivery Mechanism & Timeline:** Any CPS project will feature as part of Nezasa's regular software development and delivery processes. Nezasa's current and binding processes will govern the initial inception and delivery which can be found on

<https://support.nezasa.com/hc/articles/4402964863889-Delivery-Mechanism-Timeline>

Due to Nezasa's approach to developing and delivering new Platform capabilities and the varying scope and nature of a project any timelines are best-efforts only.

**Software Development:** Constitutes a combination of designing, creating, and deploying a software-artefact. This piece of software is deployed within the Platform setup of the particular Customer and will henceforth be part of the Platform Service consumed by the Customer.

**Ongoing Support, Operations & Maintenance:** Nezasa will be responsible for operating the customer-specific software services including patching, bug fixing and upgrades caused by Nezasa internal technical changes.

**Service Level Agreement:** The newly developed capability will feature as part of the Platform once business acceptance has taken place and will be governed and served under PlatformSLA and Support SLA.

**Further Development:** Shall Customers wish to make enhancements to the delivered Custom Platform Service at some point in the future, so shall the enhancement be subject to the same terms and conditions as outlined under 4.2.1.

**Delivery & Business Acceptance:** Nezasa will inform the Customer once a Custom Platform Service has been delivered to the production environment. Upon notification, the Customer has 5 business days to submit a notification of defect in case the delivery is not as defined per Service Order. After this period, the delivery is considered as accepted.

**Development Fee:** The fee to design, create, and deploy a particular Customer Platform Service, which may include various Premium Platform Services.

**Operations Fee:** The fee to cover the ongoing support, operations and maintenance of the CPS. The fee shall amount to a monthly percentage, determined in the Service Order, of the total development cost of the Premium Professional Service.

#### 4.2.2. Accelerated Platform Service (APS)

**Accelerated Platform Service:** This Premium Platform Service is about accelerating the delivery of a particular software driven capability. This can be through the introduction of an entirely new capability or the enhancement of an existing capability. The software capability in question is one that Nezasa intends to undertake at some point in the future and there will become a regular element of the Platform Service. The nature of these capabilities is that they serve a broader use case, something Nezasa wishes to make available to a broader range of Customers subject to its own discretionary commercial terms and conditions.

**Scoping:** The scope of a particular APS is jointly agreed by both parties and captured in the relevant Service Order. Given the joint interest of both parties, the scope shall define which share of the development efforts shall be the responsibility of the requesting party and which shall relate to Nezasa.

**Delivery Mechanism & Timeline:** Any APS project will feature as part of Nezasa's regular software development and delivery processes. Nezasa's current and binding processes will govern the initial inception and delivery which can be found under

<https://support.nezasa.com/hc/articles/4402964863889-Delivery-Mechanism-Timeline>

Due to Nezasa's approach to developing and delivering new Platform capabilities and the varying scope and nature of a project any timelines are best-guess and best-efforts only.

**Software Development:** Constitutes a combination of designing, creating, and deploying a software-artefact. This piece of software is deployed within the Platform setup and will henceforth be part of the Platform Service consumed by the Customer.

**Ongoing Support, Operations & Maintenance:** Nezasa will be responsible for operating the customer-specific software services including patching, bug fixing, and upgrades caused by Nezasa internal technical changes.

**Service Level Agreement:** The newly developed capability will feature as part of the Platform once business acceptance has taken place and will be governed and served under Platform SLA and Support SLA.

**Further Development:** Shall Customers wish to make enhancements to the delivered Accelerated Platform Service at some point in the future, ahead of Nezasa's plans, so shall the enhancement be subject to the same terms and conditions as outlined under 4.2.2.

**Delivery & Business Acceptance:** Nezasa will inform the Customer once an Accelerated Platform Service has been delivered to the production environment. Upon notification, the Customer has 5 business days to submit a notification of defect in case the delivery is not as defined per Service Order. After this period, the delivery is considered accepted.

**Development Fee:** The fee to cover the management, design, creation, deployment, and correction of a particular Accelerated Platform Service project until acceptance by the customer.

**Operations Fee:** Covers the ongoing support, operations and maintenance of the CPS. The fee shall amount to a monthly percentage, determined in the Service Order, of the total development cost of the Premium Professional Service.

## 5. Terms for Third Party Services

If Customer uses third party services available on the Platform, third party supplier terms apply. Nezasa is neither responsible nor liable for the terms and conditions of third party suppliers. The third party terms include but are not limited to the following terms below. The Customer acknowledges that they have read and agree with the following:

### Google Maps Terms & Conditions

Terms of Use Maps: <https://cloud.google.com/maps-platform/terms>

Google's Terms of Service: <https://policies.google.com/terms>

Privacy: <https://policies.google.com/privacy>

Especially for data provided through our APIs, e.g. Nezasa Location API the following additional Google Maps Platform Service Specific Terms apply, which can found here:

<https://cloud.google.com/maps-platform/terms/maps-service-terms>

## 6. Data Processing Agreement (DPA)

### 6.1. Preamble

6.1.1. This Data Processing Agreement denies the responsibilities of the Parties in the area of data protection that arise from the Services provided under the Agreement and the Customer Terms of Service by Nezasa or its Suppliers. 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.

6.1.2. This Data Processing Agreement denies 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.

## 6.2. Subject Matter and Duration

6.2.1. The subject matter of the Service Order(s) or Agreement results from the Agreement.

6.2.2. The duration of the applicable Service Order(s) or Agreement (term) corresponds to the duration of the Agreement.

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

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

6.3.2. 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 EU Model Clauses or any applicable alternative transfer mechanism as described above.

6.3.3. 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)



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

- Employees of the Customer
- Travel agents

#### **6.4. Lawful Collection**

6.4.1. 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.

#### **6.5. Technical and Organisational Measures**

6.5.1. 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.

6.5.2. 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).

6.5.3. 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.

#### **6.6. Rectification, Restriction and Erasure of Data**

6.6.1 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.

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

## 6.7. Quality Assurance and Other Duties of Nezasa

6.7.1. 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. Nezasa may claim remuneration for this.
- 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.

## 6.8. Subcontracting

6.8.1. 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.

6.8.2. 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.

6.8.3. 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.

## **6.9. Supervisory Powers of Customer**

6.9.1. 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.

6.9.2. 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.

## **6.10. Communication in the Case of Infringements by Nezasa**

6.10.1. 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.

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

### **6.11. Authority of Customer to issue instructions**

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

6.11.2. 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.

### **6.12. Liability**

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

### **6.13. Deletion and Return of Personal Data**

6.13.1. Copies or duplicates of the 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.

6.13.2. 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 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.

6.13.3. 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
<p><b>a) General / Data protection management</b> Organizational Control</p>	<ul style="list-style-type: none"> <li>● All employees at the various sites receive security awareness training.</li> <li>● Different policies exist which define rules for data classification or information security.</li> <li>● mobile device management (MDM) was introduced company-wide for central administration and control</li> </ul>
<p><b>b) Physical Access Control</b> No unauthorised access to Data Processing Facilities</p>	<p><b>Nezasa Office Zurich:</b></p> <ul style="list-style-type: none"> <li>● The Zurich office is located in a building whose main entry door is secured with a secret code.</li> <li>● The office rooms are separated from the stairway with a locked door.</li> <li>● The door 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.</li> <li>● This is done for all employees upon the start of their tenure and their access is removed on their last day.</li> <li>● Employees from other offices of Nezasa may be given temporary access for the duration of their stay.</li> <li>● 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.</li> <li>● 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.</li> </ul> <p><b>Nezasa Office Lisbon:</b></p> <ul style="list-style-type: none"> <li>● The Lisbon office building has a 24/7 concierge to whom people who enter have to identify themselves.</li> <li>● All the employees are handed their own key to access the office space.</li> <li>● Employees are required to sign a key receipt for</li> </ul>

	<p>the key. Keys are given out for the duration of an employee's tenure and returned at the end of it.</p> <ul style="list-style-type: none"> <li>• Visitors register with Nezasa and are received at the entrance of the building by a Nezasa employee.</li> </ul> <p><b>Nezasa Office Chile:</b></p> <ul style="list-style-type: none"> <li>• The Chile office building has a 24/7 concierge to whom people who enter have to identify themselves.</li> <li>• The Nezasa office itself is secured with a Smart Lock with Fingerprint access.</li> <li>• The registration for the lock is done for all employees upon the start of their tenure and their access is removed on their last day.</li> <li>• Employees from other offices of Nezasa may be given temporary access for the duration of their stay.</li> <li>• To gain access to the premises, visitors need to register at the main entry door, the concierge calls the office to inform about the visitor and the visitors are then received at the office door by an employee of Nezasa.</li> </ul>
<p><b>c) Electronic Access Control</b>          No unauthorised use of the Data Processing and Data Storage Systems</p>	<ul style="list-style-type: none"> <li>• Access to workstations and notebooks is protected via individual user accounts.</li> <li>• Access to servers is protected via separate administrator accounts.</li> <li>• The circle of authorized persons is limited to the operationally necessary extent.</li> <li>• 2-factor authentication using an authenticator App is enforced for critical systems that handle personal identifying data.</li> <li>• Nezasa has an authorization concept that is documented in written form.</li> <li>• Employees have personal accounts that can be revoked at any time.</li> <li>• 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</li> </ul>

	<p>letters.</p>
<p><b>d) Internal Access Control</b>                  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</p>	<ul style="list-style-type: none"> <li>● Access authorizations are assigned in the applications on a role-based basis. The principle of "need-to-know" and "need-to-do" is applied.</li> <li>● Role-based distinction is made between write, read and delete authorizations.</li> <li>● Each authorized user can only access data that he or she needs to perform the assigned tasks and functions.</li> <li>● Binding written regulations exist for handling access data.</li> <li>● There are no local deployments of sensitive Customer Data.</li> <li>● Nezasa has an authorization concept that is documented in written form.</li> <li>● All Nezasa-internal software implements the authorization concept.</li> <li>● Employees have personal accounts that can be revoked at any time.</li> <li>● The number of system administrators is reduced to the minimum (only engineering management).</li> <li>● When an employee leaves Nezasa, it is ensured that all accounts and permissions are revoked immediately (with a checklist).</li> <li>● Nezasa does not store personal data on paper.</li> </ul>
<p><b>e) Isolation Control</b>                  Isolated Processing of Data, which is collected for differing purposes</p>	<ul style="list-style-type: none"> <li>● Separation of production, test and development systems with separate application instances and databases.</li> <li>● Dedicated permissions for the production system.</li> <li>● Logical isolation of data by implementation of a multi-tenancy concept.</li> <li>● Accessing data of other tenants is prevented by the system.</li> </ul>

<p><b>f) Pseudonymisation</b>                  (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.</p>	<ul style="list-style-type: none"> <li>On testing &amp; development systems, Customer Data is pseudonymized.</li> </ul>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------

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

CONTROL	IMPLEMENTED MEASURES
<p><b>a) Data Transfer Control</b>                  No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport</p>	<ul style="list-style-type: none"> <li>Communication between the System of Nezasa, the Customer and third parties is encrypted (HTTPS).</li> <li>Nezasa maintains a data retention policy.</li> <li>All data storage on Nezasa computers is encrypted.</li> <li>Paper is destroyed according to DIN/EN/ISO 66399 security level P-4 with a shredder in the office.</li> </ul>
<p><b>b) Data Entry Control</b>                  Verification, whether and by whom Personal Data is entered into a Data Processing System, is changed or deleted</p>	<ul style="list-style-type: none"> <li>The objects contain the following attributes that must be updated with each change:                         <ul style="list-style-type: none"> <li>Author</li> <li>Creation timestamp</li> <li>Author of the modification</li> <li>Modification timestamp</li> </ul> </li> <li>The technical attributes can be read from the database by Nezasa.</li> <li>The most current value of the attributes can be visible in the backup application (e.g. last modified).</li> <li>Automated, daily backups are created for all data to enforce traceability.</li> </ul>

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

CONTROL	IMPLEMENTED MEASURES
---------	----------------------



<p><b>a) Availability Control</b> Prevention of accidental or wilful destruction or loss; Rapid Recovery (Art. 32 Abs. 1 lit. c GDPR)</p>	<ul style="list-style-type: none"> <li>• The data center of the service provider Amazon AWS in Dublin (Ireland) has been certified according to ISO 27001, ISO 27017 and ISO 27018.</li> <li>• 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.</li> <li>• For more details see AWS TOM.</li> <li>• Backups of the data stored on AWS are carried out daily and stored on a secondary cloud provider according to an internal retention policy.</li> </ul>
-----------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

CONTROL	IMPLEMENTED MEASURES
<p>a) Data Protection Management</p>	<ul style="list-style-type: none"> <li>• Data protection is a regular agenda item at management meetings. The corresponding discussions and decisions are logged in a data protection log.</li> <li>• 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.</li> </ul>
<p>b) Contract Supervision</p>	<ul style="list-style-type: none"> <li>• All employees handling personal data have committed themselves to confidentiality.</li> <li>• Processing solely under and according to data processing agreement and subject to directives from our customers</li> </ul>

**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: 2010 Standard Contractual Clauses for the Transfer of Personal Data From the Community to Third Countries (Controller to Processor transfers)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection Nezasa AG, (hereinafter "data importer"), under a mandate from Customer (hereinafter the "data exporter") each a "party"; together "the parties", HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex 1.

#### **Clause 1: Definitions**

For the purposes of the Clauses:

- a. **'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority'** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- b. **'the data exporter'** means the controller who transfers the personal data;
- c. **'the data importer'** means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring

adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

- d. **'the subprocessor'** means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- e. **'the applicable data protection law'** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- f. **'technical and organisational security measures'** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

## Clause 2: Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

## Clause 3: Third party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if

the data subject so expressly wishes and if permitted by national law.

#### **Clause 4: Obligations of the data exporter**

The data exporter agrees and warrants:

- a. that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- b. that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- c. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- d. that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- e. that it will ensure compliance with the security measures;
- f. that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- g. to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- h. to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- i. that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- j. that it will ensure compliance with Clause 4(a) to (i).

#### **Clause 5: Obligations of the data importer**

The data importer agrees and warrants:

- a. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- b. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- c. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- d. that it will promptly notify the data exporter about:
  - a. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
  - b. any accidental or unauthorised access, and
  - c. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
  - d. to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
  - e. at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
  - f. to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
  - g. that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
  - h. that the processing services by the subprocessor will be carried out in accordance with Clause 11; i. to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

## Clause 6: Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

#### **Clause 7: Mediation and jurisdiction**

1. The data importer agrees that if the data subject invokes against its third party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject: a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority; b. to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

#### **Clause 8: Cooperation with supervisory authorities**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection

law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

### **Clause 9: Governing Law**

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

### **Clause 10: Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

### **Clause 11: Subprocessing**

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to full its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and noticed by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

**Clause 12: Obligation after the termination of personal data processing services**

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.



## Previous Versions

Below are listed the previous versions of our Customer Terms of Service with the dates that they were published.

If your Product Plan or Support Plan are not applicable to the parameters stipulated above, please refer to the most recent version of this contract where parameters for your agreed Product Plan or Support Plan are outlined.

Version October 31st 2022: <https://nezasa.com/customer-terms-of-service-october-2022/>