AviLabs Data Processing Addendum

This Data Processing Addendum ("**DPA**") supplements the Plan3 Customer Agreement available at https://www.plan3.aero/terms, or other agreement between Customer and AviLabs governing Customer's use of the AviLab's service offerings, when the GDPR applies to its use of the AviLab's Services to process Customer Data. This DPA is an agreement between the entity you represent ("**Customer**", "**you**" or "**your**") and AviLabs.

This DPA sets out the terms that apply when Customer's Data is processed by AviLabs and its purpose is to ensure such processing is conducted in accordance with Applicable Law and respects the rights of individuals whose personal data are processed under the Customer Agreement.

All capitalized terms used in this DPA but not defined will have the meaning set forth in the Customer Agreement. To the extent of any conflict or inconsistency between this DPA, any previously executed data processing agreement, and the remaining terms of the Customer Agreement, this DPA will govern.

1 Definitions

"**Controller**", "**Processor**", "**Personal Data**", "**Data Subject**" and "**Processing**" have the meanings given under the GDPR (and "Process", "Processed" and "Processes" shall be construed accordingly);

"**Customer Agreement**" shall mean the contract between the Data Controller and the Data Processor pursuant to which the Data Processor performs Data Processing;

"**Customer Personal Data**" means Personal Data Customer uploads or otherwise inputs into the Service and which is processed in connection with the provision of the Service under the Customer Agreement by AviLabs on behalf of the Customer.

"**Data Breach**" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data processed by AviLabs and/or its Sub-processors in connection with the provision of the Service.

"**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

"**Services**" means services provided by AviLabs under the Customer Agreement.

"**Sub-processor**" means any person or entity engaged by Processor that Processes Customer Personal Data to help provide the Services.

2 Relationship of the Parties

2.1 The Parties acknowledge and agree that with regard to Customer Personal Data, Customer is a Controller and AviLabs is a Processor.

2.2 Each Party wishes to ensure compliance with applicable laws apply to each Party and to perform its obligations under this DPA in a manner that does not cause the other Party to breach any data protection laws, including the GDPR. Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR.

3 Processing

3.1 Annex 1 to this DPA sets out the scope, nature and purpose of processing by the Provider, the duration of the processing and the types of Personal Data and categories of Data Subject.

3.2 AviLabs shall in respect of all Personal Data that it Processes on behalf of the Customer, that at all times:

3.2.1 it shall Process such Personal Data only for the purposes of providing the Services and as may subsequently be agreed between the Parties in writing and, in so doing, shall act solely on the reasonable and lawful instructions of the Controller in accordance with Section 4;

3.2.2 it shall not Process, apply, or use, the Personal Data for any purpose other than as required and necessary to provide the Services, unless otherwise expressly permitted under the Customer Agreement;

3.2.3 comply with all applicable data protection legislation in the Processing of Personal Data; and

3.2.4 ensure that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential.

4 Customer's Instructions

4.1 Customer, as a Data Controller, appoints AviLabs as a Data Processor to process Customer Personal Data on behalf of, and in accordance with, Customer's instructions (as defined below). Customer will not instruct AviLabs to process Customer Personal Data in violation of applicable law. AviLabs will promptly inform Customer if, in AviLab's's opinion, an instruction from Customer infringes applicable law.

4.2 The Customer Agreement, including this DPA, along with Customer providing instructions via tools such as the Plan 3 Platform made available by AviLabs for the Services, constitutes Customer's documented instructions to AviLabs regarding the processing of Customer Personal Data, unless otherwise agreed in writing.

5 The Controller's Obligations

5.1 The Customer, as the Data Controller, warrants that it has the right to process the personal data in question and that it has ensured that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to AviLabs for the duration and purposes of this agreement

5.2 The Customer shall be responsible for notifying Processing activities to the Data Protection Authority and acquiring a permit for the Processing, where applicable.

5.3 The Customer acknowledges and undertakes that it:

5.3.1 will, in order to use some of the Services, provide AviLabs with such Personal Data as is necessary to provide the Services to Customer in accordance with this DPA;

5.3.2 is responsible for complying with all data protection laws applicable to the Customer and AviLabs will support the Customer in doing so, according to the terms of this DPA;

5.3.3 has implemented appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with applicable law, including the GDPR.

6 Sub-processing

6.1 Customer acknowledges and agrees that certain third parties may be retained as Sub-Processors to process Customer Personal Data on AviLab's behalf in order to provide the Service. AviLab's current Sub-processors can be found in Annex 3 to this DPA.

6.2 Customer will be notified of new Sub-Processors ten (10) business days before AviLabs authorizes such Sub-Processor to process Customer Personal Data (or in the case of an emergency, as soon as reasonably practicable).

6.3 Avilabs will impose contractual obligations on any Sub-Processor AviLabs appoints requiring it to protect Customer Personal Data to standards which are no less protective than those set forth under this DPA. AviLabs remains liable for its Sub-Processor's performance under this DPA to the same extent AviLabs is liable for its own performance.

6.4 To object to a new Sub-Processor, Customer can either terminate the Customer Agreement (and this DPA) pursuant to its terms or cease using the Service for which AviLabs has engaged the Sub-processor (where possible).

7 Security

7.1 AviLabs shall ensure that appropriate technical and organisational measures are implemented and maintained, to the extent that such measures are the responsibility of the AviLabs, against unauthorised or unlawful Processing of, or accidental loss, destruction or damage to, Personal Data to ensure a level of security appropriate to the risk. Such measures will take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, so as to ensure a level of security appropriate to the risk. Generally, such required technical/organizational measures include, without limitation;

7.1.1 the encryption and (where possible) the pseudonymisation of Personal Data;

7.1.2 the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and Services;

7.1.3 the ability to restore the availability of and access to Personal Data in a timely manner in the event of physical and/or technical incident; and

7.1.4 the introduction and maintenance of a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

Without limiting the foregoing, AviLabs shall implement technical and organisational measures that are acknowledged and hereby accepted by the Customer as referred to in Annex 2 which shall become part of this DPA.

8 Data Subject Rights and Requests

8.1 The Customer, as the Data Controller, is responsible for protecting the rights of Data Subjects as provided in Chapter 3 of the GDPR. AviLabs shall assist the Customer to facilitate the fulfilments of his obligations to respond to requests for exercising Data Subject´s rights laid down in applicable data protection laws.

8.2 To the extent legally permitted, AviLabs will promptly notify the Customer, or refer the individual back to the Customer, if AviLabs receives any requests from an individual seeking to exercise any rights afforded to them under applicable law regarding their personal data, which may include: subject access rights, rights to rectification, restriction of processing, data portability, the right to object to processing and automated decision-making. AviLabs shall not otherwise answer that Data Subject Request except on the instruction of the Customer, unless otherwise required by data protection laws.

8.3 In the event Customer is unable to address a Data Subject Request in its use of the Service, AviLabs will, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent AviLabs is legally permitted to do so and the response to such Data Subject Request is required under Applicable Law.

9 Reporting of Personal Data Breaches

9.1 AviLabs will comply with any Data Breach related obligations applicable to it under applicable law.

9.2 AviLabs shall notify the Customer without undue delay upon AviLabs becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed (Data Breach).

9.3 Furthermore, AviLabs will assist Customer by notifying it of a confirmed Data Breach without undue delay or within the time period required under applicable law, and in any event no later than fourty-eight (48) hours following such confirmation. To the extent available, this notification will include AviLabs's assessment of the following:

9.3.1 description of the nature of the Data Breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

9.3.2 the likely consequences of the Data Breach; and

9.3.3 description of the measures taken or proposed to be taken by AviLabs to address the Data Breach, including, where applicable, measures to mitigate its possible adverse effects.

9.4 Following a Data Breach, AviLabs shall provide timely and periodic updates to Customer as additional information regarding the Data Breach becomes available. Customer acknowledges that any updates and the notification under Section 9.3 may be based on incomplete information.

9.5 AviLabs shall co-operate with Customer and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each the Personal Data Breach. The Customer, as the Data Controller, is responsible for and has the sole right to determine (subject to applicable law):

9.5.1 whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

9.5.2 whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

9.6 Notifications under this Section 9 will be delivered to one or more of Customer's contacts by any means AviLabs selects, including via email. It is Customer's sole responsibility to ensure Customer's point of contacts maintain accurate contact information on the Plan 3 Platform at all times.

9.7 Nothing in this DPA will be construed to require AviLabs to violate, or delay compliance with, any legal obligation it may have with respect to a Data Breach or other security incidents generally.

10 Supervisory Authorities or other Regulatory Authorities

10.1 AviLabs shall immediately notify the Customer if any complaint, enquiry or investigation is made (including by any Supervisory Authority) relating to the AviLab's Processing of Personal Data under this DPA, unless prohibited from doing so by applicable laws or by a regulatory authority.

10.2 AviLabs shall provide reasonable assistance to, and cooperate with the Customer, to enable the Customer to investigate and comply with any such complaint, enquiry or investigation.

10.3 The Customer will manage all communications or correspondence with the supervisory authority in relation to the Processing of Customer Personal Data or this DPA, unless the the Customer notifies AviLabs, or the supervisory authority asks in writing to deal directly with AviLabs, in which case the AviLabs will do so in consultation with the Customer, as permitted by applicable law.

10.4 AviLabs will provide reasonable assistance to Customer for Customer's performance of any legally required data protection impact assessment of the processing or proposed processing of Customer Personal Data involving AviLabs, and in consultation with supervisory authorities or other regulatory authorities as required, by providing Customer with any publicly available documentation for the Service or by complying with Section 11 (Audits) below. Additional support for data protection impact assessments may require AviLabs to charge the Customer for such assistance, provided however that the parties shall agree on the fees associated, the scope of AviLab's involvement and other terms necessary.

11 Audits

11.1 During the term of this DPA, at the request of the Customer and subject to a duty of confidentiality, AviLabs shall allow for and contribute to audit conducted by the Customer, or another auditor appointed by the Customer, of documentation, certifications, data, reports, and records relating to AviLabs's processing of Customer Personal Data for the sole purpose of determining AviLabs's compliance with this DPA and the data protection laws that apply to AviLabs, subject to the terms of this Section 11 ("Audit").

11.2 The Customer may request an Audit upon fifteen (15) days' prior written notice to AviLabs, no more than once annually, except, in the event of a Data Breach occurring by AviLabs or when an Audit is imposed on the Customer by a supervisory authority, in which case Customer may request an Audit within a reasonable period of time following such Data Breach or such request from a supervisory authority.

11.3 To the extent that an Audit does not provide sufficient information to allow Customer to determine AviLabs's compliance with the terms of this DPA or applicable law, Customer may require access to AviLabs's premises, systems and employees (an "Inspection") subject to the parties having mutually agreed upon (a) the scope, timing, and duration of the Inspection, (b) the use of an Auditor to conduct the Inspection, and (c) the Inspection being carried out only during AviLabs's regular business hours, with minimal disruption to AviLabs's business operations.

11.4 In connection with any Audit or Inspection conducted in accordance with this Section 11, auditor must be bound by obligations of confidentiality. Auditor's will not be entitled to receive any data or information pertaining to other customers of AviLabs or any other Confidential Information of AviLabs that is not directly relevant for the authorized purposes of the Audit or Inspection.

11.5 All costs associated with an Audit or an Inspection under this Section 11 shall be borne by the Customer. However, AviLabs shall bear its own respective costs of assisting with the Audit or the Inspection.

12 Data Transfer

12.1 AviLabs may transfer or authorize the transfer of Personal Data to countries outside the EU and/or the European Economic Area (EEA) if appropriate safeguards in relation to transfer have been made. The Parties agree that to achieve this, AviLabs shall rely on the EU approved standard contractual clauses for the transfer of personal data, in the form approved by the European Commission (the "Model Clauses"), by procuring that such recipient of Personal Data (i.e. any non EU/EEA Sub Processor) enters into the standard contractual clauses or, where applicable and agreed specifically by the Customer, other measures are in place to ensure that the Personal Data is adequately protected.

13 Termination of the DPA and Destruction of Customer Personal Data

13.1 This DPA will continue in force until the termination of the Customer Agreement.

13.2 Upon termination of the Agreement and written verified request from Customer's authorized representative (which for purposes of this section is either a billing owner or an administrator of the Service or a Customer personnel who has confirmed in writing that they are authorized to make decisions on behalf of the Customer), AviLabs will delete Customer Personal Data, unless otherwise expressly stated in the Customer Agreement or prohibited by applicable law.

Annex 1 - Details of Data Processing

1. ***Subject matter of the processing of Customer Personal Data***

The subject matter of the processing of Customer Personal Data is for providing the Services, which inter alia allow the Customer to monitor their flight disruptions and offer their End Users solutions in relation to such disruptions, as set out in the Customer Agreement.

2. ***Duration of the Processing of Customer Personal Data***

AviLabs will retain and process Customer Personal Data for as long as necessary to provide the Services or as defined by the Customer Agreement.

3. ***The nature and purpose of the Processing of Customer Personal Data***

The nature and purpose of the processing of Customer Personal Data is to provide the Services as they are initiated by Customer from time to time in its use of the Service.

4. ***The types of Customer Personal Data to be processed***

The following types of Customer Personal Data are processed:

- Personal master data: customer's full name, date of birth, gender and IP address
- Communication data: customer's email, home address, phone number
- Flight information data and other travel information data

Sensitive Customer Personal Data is not specifically sought or requested for the Services. However, it is possible that the Customer Personal Data supplied to AviLabs in providing the services could include sensitive Customer Personal Data. As with all Customer Personal Data, access to data is limited to business need only, data is encrypted in transit and at rest, and data is replicated to a separate data store.

5. ***Categories of data subject to whom Customer Personal Data relates***

The Data Processing concerns the following categories of data subjects:

- End Users of the Customer (i.e. the individual travellers or passengers of the Customer)

6. ***Location of Processing of Customer Personal Data by Service Provider***

Customer Personal Data is processed by AviLabs in Iceland. *However, our Sub-processors are located elsewhere,* meaning that processing may take place elsewhere, *s*ee Sub-processor list in Annex 2,

7. ***The obligations and rights of the Data Controller***

The obligations and rights of the Data Controller are set out in this DPA and in the Customer Agreement.

Annex 2 – AviLabs Technical and Organizational Measures (TOMS)

All references to "Data" herein shall mean "Customer Personal Data"

Data Security Measures	**Data Processors technical and organisational description of measures**
Measures of pseudonymization and encryption of personal data	Technical measures that AviLabs does to have the data in a Pseudonymization manner and encrypted: - Data is encrypted in transit and encrypted at rest (and remains encrypted at rest). The connection to admin.plan.aero is encrypted with 128-bit encryption and supports TLS 1.2 and above. Logins and sensitive data transfer are performed over encrypted protocols such as TLS or ssh. - End users of AviLabs´s products need user credentials to access the product - User management is managed with top-of-the-line access management tool called Auth0: https://auth0.com/security. The tool supports many of the most commonly used methods available Today. The tool also supports MFA - Each user is given access roles within the tool as well and not give access to any personal data unless needed - Data is stored in different AZ (Availability Zones) within AWS to secure backups and restore procedures. All code that is committed for changes in regards of personal data is code reviewed by at least one other employee
Measures to ensure confidentiality	**Technical measures for physical access control (preventing unauthorised access to premises and facilities where processing is carried out)** Regarding Office: - In general, the office is protected and secured through access control systems (smart card access system which allows for traceability and management of access, see further below). - Furthermore, the buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance and intruder alarm systems. Regarding Product/software: - Physical access control is managed by using a top-of-the-line access control system called auth0 Regarding Data centres: - Plan3 uses Amazon Web Services (AWS) to provide management and hosting of production servers and databases in European Union. AWS employs a robust physical security program with multiple certifications, including SSAE 16 and ISO 27001 certification. For more info regarding procedures regarding our data centers please visit https://aws.amazon.com/compliance/data-center/controls/ - All Data Centres have strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Centre facilities from being compromised. Only authorized

	representatives have access to systems and infrastructure within the Data Centre facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis. - All third-party Data Centre providers log the names and times of authorized personnel entering the Data Centres. **Technical measures for system access control (technical measures (keyword/password protection) and organizational measures (user master data set) for user identification and authentication, preventing unauthorised access to Processing systems)** - All users of Plan3 need to access the processing system with a unique identifier (user ID) - AviLabs has strict password rotation policies for users with minimum of 8 character-, lower and upper-case letter, numbers and special characters - Security patches/updates are done as soon as they arise **Technical measures for data access control (access authorization and data access rights granted on need-to-know basis, as well as monitoring and tracking access; that shall ensuring that persons authorised to use a data processing system have access only to the data to which they have authority, and that Personal Data cannot otherwise be read, copied, modified or removed in the course of processing or use and while being stored)** - Only Developers with AWS access keys and Multi Factor Authentication can access the data from the server side - All personal data is stored in secure data centres in Ireland hosted by AWS. All data is encrypted at rest. Access to data is restricted and only data admins can access it with IAM roles from AWS and by using MFA. - All production servers are operated in the Data centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. - All access authorization is handled in infrastructure code. - All changes to the infrastructure code is code reviewed by another person to secure the changes are up to security standards - All changes are logged and monitored with tool sets that AviLabs has established. Traceability is available as well with separate tools **Technical measures for separation control (measures which shall ensure that data collected for different purposes can be Processed separately)** - AviLabs uses the technical capabilities of the deployed software (for example: multitenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers. - Customers (including its Controllers) have access only to its own data.
Measures for the protection of data during transmission	- Personal Data is encrypted in transit and encrypted at rest (and remains encrypted at rest). The connection to admin.plan3.aero is encrypted with 128-bit encryption and supports TLS 1.2 and above. Logins and sensitive data transfer are performed over encrypted protocols such as TLS or ssh.

	- When data is transferred between Plan3 and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of AviLabs´s controlled network
Measures for the protection of data during storage	- Personal Data is stored encrypted and backed up. Data backups are encrypted. Personal data is encrypted at rest with AES 256 bit secret keys.
Measures for ensuring events logging	- AviLabs only allows authorized personnel to access Personal Data as required in the course of their duty. - AviLabs has implemented a logging system for input, modification, and deletion, or blocking of Personal Data by AviLabs or its sub processors within the Cloud Service to the extent technically possible - All access to information security management systems at Asana are restricted, monitored, and logged. At a minimum, log entries include date, timestamp, action performed, and the user ID or device ID of the action performed. The level of additional detail to be recorded by each audit log will be proportional to the amount and sensitivity of the information stored and/or processed on that system. All logs are protected from change.
Measures for ensuring availability and resilience of processing systems and services	- All data is stored in a high availability setup in AviLab´s data centres - Disaster recovery plans are in place and are run regularly to ensure the integrity of the data - Data is stored in different availability zones within AWS to ensure access if one AZ goes down. - AviLab's shall ensure that penetration testing is performed by a qualified third party on an annual basis - AviLab shall conduct periodic risk assessments of all systems and networks that process Data on at least an annual basis; - AviLabs shall monitor for security incidents and maintain a remediation plan to ensure timely fixes to any discovered vulnerabilities; AviLab's shall ensure that it has the resources responsible for information security efforts - Data Subject Access Requests and requests regarding the "right to be forgotten" are handled individually
Measures to restore availability and access to personal data in the event of a technical incident	- Data is stored in a managed service by AWS called DynamoDB. Backups are done daily and also as Point In Time Restore (PITR). Disaster recovery plans are in place to restore data and fire drill are run regularly - Data is also stored in a „Master/Slave" setup (i.e. where the Master Database instance fails, there is a database replica running as slave that can be promoted to be the master database quickly and efficiently) in databases hosted in AviLabs´s data centres. - Daily backups are taken automatically from all databases. - Retention period of each backup is 30 days

	- Backups are encrypted and have the same protection in place as production
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	- AviLabs has procedures and processes for regular testing, and evaluating its technical and organizational measures. In particular, AviLabs shall use the following to implement the control and measure sections described above in this document: regular internal evaluation of its security procedures (inter alia on AviLabs incident response management procedures) and external and internal penetration testing and/or regular external audits to prove those security measures
Measures for ensuring accountability	- The transfer of Personal Data to a third party (e.g. customers, sub-contractors, service providers) shall only be made if a corresponding contract exists, and only for the specific purposes. Furthermore, if Personal Data is transferred to companies located outside the EEA, the Processor provides that an adequate level of data protection exists at the target location or organisation in accordance with the European Union's data protection requirements, e.g. by employing contracts based on the Standard Contractual Clauses. - No third party data processing will be done, as per Article 28 GDPR, without the corresponding instructions from the data controller, e.g.: clear and unambiguous contractual arrangements.

Annex 3 - List of existing Sub-processors

This list identifies our current Sub-processors:

Name of processor	**Location**	**Type of data processed**	**Derogation for international transfer**
Amazon AWS	EU	Customer Personal Data, for cloud computing, web services and data storage.	N/A
Twilio Inc.	USA	SMS message data and mobile phone numbers of End Users	Standard contractual clauses.