AZUL S.A.
Brazilian Publicly Held Company
CNPJ/ME No. 09.305.994/0001-29
NIRE 35.300.361.130

DATA PROTECTION AND INFORMATION SECURITY POLICY FOR THIRD PARTIES

This Data Protection and Information Security Policy for Third Parties ("Policy") establishes the principles, guidelines, and minimum standards of conduct to be observed by Third Parties (as defined below). This Policy shall be observed by all Third Parties, unless otherwise provided by contract. In the event of a conflict between the provisions of this Policy and the Contract, the Third Party shall observe the provisions set forth in the Contract, which, for all purposes, shall prevail in its relationship with Azul.

1. DEFINITIONS

For the purposes of this Policy, the following definitions shall have the meanings assigned below:

a) Collaborators: partners, officers, managers, employees, service providers, business partners and/or any other similar persons linked to the Third Party.

b) Contract: the agreement in force between Azul and the Third Party.

c) Controller: the natural person or legal entity responsible for decisions regarding the processing of Personal Data within the scope of the Contract.

d) Personal Data: any information, within the scope of the Contract, related to an identified or identifiable natural person (e.g., name, IP address, government IDs, location data, etc.).

e) Azul: any entities and business units of the Azul group, notably: Azul S.A., Azul Linhas Aéreas Brasileiras S.A., IntelAzul S.A., Azul Viagens, Azul Logística, Azul Fidelidade, and Azul Conecta.

f) Third Party: a supplier, service provider, or business partner that processes Personal Data within the scope of the Contract, as qualified in the Contract.

g) Processor: the natural person or legal entity that processes Personal Data on behalf of the Controller within the scope of the Contract.

h) Data Subject: the person to whom the Personal Data refers, including Azul's or third parties' customers and crew members, within the scope of the Contract.

2. PURPOSES

This Policy is intended to regulate the processing of Personal Data carried out by the Third Party within the scope of its relationship with Azul. For purposes of this Policy, the Third Party may act as Controller or Processor, as defined in the Contract, pursuant to Law No. 13,709/2018 ("LGPD"). This Policy shall be read together with Azul's Code of Conduct for Business Partners.

3. PRINCIPLES

When processing Personal Data, the Third Party must observe the following principles:

a) Purpose Limitation: the processing of Personal Data must serve legitimate, specific, explicit purposes that are informed to the Data Subjects, and any subsequent processing incompatible with such purposes is prohibited. If the Third Party acts as Processor in relation to the Personal Data, the purposes for using such data will be defined by Azul itself, and the Third Party, through its legal representative(s) and Collaborators, must follow the instructions received.

b) Adequacy: the processing of Personal Data must be compatible with the purposes informed to the Data Subject, according to the context of the processing. The Third Party must make every effort to ensure that no Personal Data is processed beyond what has been instructed by Azul.

c) Minimization: the processing must be limited to the minimum Personal Data effectively necessary to meet the purposes of the Third Party and/or Azul, restricted to Personal Data that is relevant, proportional, and not excessive. The Third Party must instruct its Collaborators not to collect, store, or otherwise process Personal Data excessively or unnecessarily. Personal Data must always be processed to comply with contractual provisions, so that if the Third Party does not need certain information, it must not request or use it. The Third Party must ensure that its Collaborators authorized to process Personal Data in connection with the performance of the Contract will be granted access to Personal Data only to the extent strictly necessary.

d) Free access: the Data Subject must have facilitated and free access to information regarding the form and duration of the processing of Personal Data, as well as the entirety of their Personal Data. If the Third Party receives any request in this regard involving the processing of Personal Data under the Contract, it must proceed as established in this Policy and/or in the Contract.

e) Data quality: the Personal Data must be accurate, clear, relevant, and up to date, according to the need and for the fulfillment of the purpose of its processing. The Third Party must inform Azul if it becomes aware of any inaccuracy related to Personal Data, and must also train its Collaborators, when necessary, to properly register Data Subjects in the systems.

f) **Transparency:** Data Subjects must receive clear, accurate, and easily accessible information about the processing of their Personal Data. To that end, the Third Party must maintain, at a minimum, a privacy policy or notice that is publicly accessible to the Data Subject.

g) **Security:** Personal Data must be protected against unauthorized access and against accidental or unlawful situations involving destruction, loss, alteration, communication, or dissemination, through technical and administrative measures. The Third Party must adopt the security measures set forth in this Policy and in any other manuals or instructions provided by Azul, in addition to establishing appropriate access controls for Personal Data. Access to Personal Data must be properly recorded through a detailed inventory containing, for example, the date, time, and name of the person responsible for accessing the Personal Data. This inventory may be audited by Azul, pursuant to the Contract.

h) **Prevention:** damages arising from the processing of Personal Data must be prevented. To that end, in addition to complying with the provisions of applicable law and this Policy, the Third Party must keep its Collaborators continuously trained, adopting best privacy governance practices, and must conduct formal training at least once per year and keep updated records of the training sessions carried out, including dates, content, and participants.

i) **Non-Discrimination:** Personal Data may not be processed for unlawful or abusive discriminatory purposes. The Third Party must always be attentive to the possibility that a given processing activity may be considered discriminatory and, in that case, must immediately report it to Azul so that Azul may assess the possibility of risk mitigation and the need to interrupt the processing, in compliance with Azul's Code of Ethics and Conduct.

j) **Accountability:** the Third Party shall keep its records of Personal Data processing activities up to date, including which Personal Data is processed, with whom it is shared, the software used, the locations where it is stored, the source of the Personal Data, and when and how it is discarded. In addition, the Third Party must cooperate with Azul, if requested, in the preparation of other documents necessary for proper governance, such as data protection impact assessments (DPIAs) or legitimate interest assessments (LIAs).

4. DATA SUBJECT RIGHTS

Data Subjects have a series of rights related to their Personal Data, as provided by law and duly explained in Azul's Privacy Policy. No right is absolute, and requests must be analyzed individually, considering the context and interactions of that Data Subject with Azul and the Third Party. If the Third Party receives any request from a Data Subject related to their Personal Data, the Third Party must refrain from responding and must immediately direct the request to

privacy@voeazul.com.br or refer the Data Subject to the Privacy Portal, unless the Contract or Azul expressly authorizes it to respond to the Data Subject.

The main rights provided by law are described below, indicating what may be requested or required by Data Subjects:

Right	Details
Confirmation and access	The Data Subject may request confirmation as to whether their Personal Data is being processed and, if so, may request access to such Personal Data, including copies of the records we maintain about them.
Anonymization, blocking, or deletion	The Data Subject may request (a) the anonymization of their Personal Data, so that such data can no longer be related to the Data Subject; (b) the blocking of Personal Data, temporarily suspending the possibility of processing for certain purposes; and (c) the deletion of Personal Data.
Correction	The Data Subject may request the correction of their Personal Data if it is incomplete, inaccurate, or outdated.
Information on the possibility of not consenting	The Data Subject has the right to receive clear and complete information about the possibility and the consequences of not providing consent when consent is requested.
Information on data sharing	The Data Subject has the right to know the public and private entities with which their Personal Data is shared.
Objection	When data processing occurs under a legal basis that does not require consent, the Data Subject may object to the processing and request that it be stopped.
Portability	The Data Subject may request that their Personal Data be provided in a structured and interoperable format for transfer to a third party, provided that such transfer does not violate intellectual property or any trade secret.
Withdrawal of consent	If the Data Subject has provided consent for data processing, they may choose to withdraw that consent.

5. DATA SHARING

The Third Party guarantees that Personal Data will be disclosed or shared only with authorized subcontractors and other third parties, exclusively to meet the processing purposes provided for in the Contract. In such cases, the Third Party must ensure that such recipients observe, at a minimum, the same security, governance, and confidentiality standards provided for in this Policy and in the Contract, entering into specific data processing terms whenever applicable, as well as adopting continuous monitoring mechanisms to verify and ensure compliance with these standards by subcontractors, including periodic assessments and requests for evidence when necessary. The Third Party further undertakes to keep an updated record of all third parties with

whom it shares Personal Data related to the Contract and to make such information available upon Azul's request.

6. MONITORING AND AUDIT

Azul may, at its sole discretion and upon prior notice, conduct audits, inspections, compliance assessments, or requests for evidence related to the processing of Personal Data carried out by the Third Party with respect to the guidelines of this Policy and the Contract, including, when appropriate, requesting reports or documentation on the maturity of the Third Party's information security program.

The Third Party must fully cooperate during such procedures, ensuring access to relevant information and implementing any corrective measures within the deadlines defined.

7. INFORMATION SECURITY

The Third Party is responsible for its use of Personal Data, which must follow the guidelines of this Policy and information security best practices throughout the entire processing life cycle.

The following rules must be observed to ensure an adequate level of information security, as applicable to the Contract:

a) **Security Governance and Compliance:** The Third Party must maintain cybersecurity policies, standards, and processes applied throughout its group, ensuring their continuous execution. It must also ensure that subcontractors comply with security guidelines equivalent to those required by this Policy.

b) **Data Handling:** The Third Party must take the utmost care in its use of Personal Data, ensuring that notes are not left, and documents containing such information are not handled, in circulation areas such as meeting rooms or public spaces.

c) **Systems:** The Third Party must primarily use systems approved by Azul for the processing of Personal Data. The following are prohibited: (i) using standalone spreadsheets, contact lists on personal cell phones, and paper notebooks and forms for the processing of Personal Data, unless authorized by Azul; (ii) using the approved systems for personal purposes; (iii) deleting, modifying, copying, transferring, reverse engineering, or granting access to the systems to third parties not authorized by Azul; and (iv) using the system together with any software not licensed or not authorized by Azul.

d) **Password and Access Management:** The Third Party must ensure that its Collaborators use strong, unique passwords kept confidential, observing, at a minimum, appropriate complexity requirements, periodic credential updates, and mandatory use of multi-factor authentication whenever available. The use of generic or shared accounts or the disclosure of access credentials is prohibited, unless expressly authorized by Azul. Access privileges must follow the principle of least privilege, with access granted only to the

extent strictly necessary for the performance of duties. The Third Party shall inform Azul, without undue delay, whenever an account is no longer necessary.

e) **Devices and Storage:** The Third Party's Collaborators must use appropriately protected devices, observing, at a minimum, updated operating systems with critical patches applied, active antivirus and antimalware solutions, and encrypted hard drives and storage units. Strong encryption must be used for all Personal Data in transit and at rest, and the use of personal devices (BYOD) is prohibited without Azul's authorization. Any local storage must be exceptional and protected by appropriate mechanisms.

f) **Use of Devices Provided by Azul:** If Azul provides the Third Party with any devices, systems, equipment, or technological tools to perform the activities provided for in the Contract, the Third Party must use them exclusively for professional purposes related to the Contract, fully observing the policies, standards, technical requirements, and use restrictions defined by Azul. The Third Party must keep such devices in its custody, safeguard their integrity, and immediately notify Azul of any loss, damage, malfunction, or suspicion of misuse.

g) **Centralized Event Logging:** The Third Party must maintain a centralized logging process for events related to the detection, prevention, and response to malware, including alerts generated by antivirus, antimalware, and antispyware solutions, in order to enable continuous monitoring, incident correlation, and verification of the effectiveness of protection controls.

h) **Physical Environment:** The Third Party must ensure appropriate physical controls to prevent improper access, such as: use of access cards or equivalent mechanisms to enter facilities where Personal Data is stored, physical access monitoring or logging, prohibition of unnecessary printing containing Personal Data, and secure disposal of documents.

i) **Log Recording and Monitoring:** The Third Party must maintain complete logs of access to, changes to, deletion of, and movement of Personal Data. Records must be protected against alteration and kept for a period consistent with the Contract, and Azul may request them at any time.

j) **Change Management:** The Third Party must ensure that any changes to systems, configurations, infrastructure, applications, processes, or technological components used for the processing of Personal Data are submitted to formal change management procedures, including, at a minimum, prior assessment of security impact, documentation of the changes made, appropriate approval before implementation, and the testing necessary to ensure that information security or operational continuity is not compromised.

k) **Security Testing:** Periodically or upon Azul's request, as applicable to the Contract, the Third Party must perform pentests, vulnerability analyses, hardening reviews, and risk

assessments on new systems or processes that process Personal Data. The results must be documented and made available to Azul upon request.

l) **Protection Against Social Engineering:** The Third Party must maintain an ongoing awareness and training program for its Collaborators regarding risks such as phishing and other social engineering techniques, in order to reduce the likelihood of incidents resulting from human error.

m) **Backups and Business Continuity:** The Third Party must maintain adequate backup and data recovery mechanisms, ensuring integrity, availability, and operational resilience. Backups containing Personal Data must be encrypted and accessible only to authorized Collaborators.

n) **Offboarding, Role Change, and Loss of Access:** In the event of termination of the Collaborator's relationship with the Third Party, or if there is a change in the Collaborator's role that eliminates the need for access to the data, the Third Party must take the appropriate measures to revoke such Collaborator's access to Personal Data. In the event of termination, the Third Party must also request that the Collaborator return any and all work devices in their possession.

8. COMMUNICATIONS AND INCIDENT REPORTING

If the Third Party becomes aware of or suspects any event that violates the rules of this Policy or places the security of Azul's Personal Data at risk, the Third Party must, within the period defined in the Contract, notify Azul of the matter by email at privacy@voeazul.com.br. To the extent possible, such notice must contain (i) the time and date on which the incident was identified; (ii) the type of information involved; (iii) the cause and extent of the incident; (iv) the context of what occurred; and (v) any additional information that may facilitate understanding of the event.

Communication regarding an incident is vital to Azul. If the Third Party fails to provide such communication, it will be in breach of this Policy.

After the initial communication, the Third Party must keep Azul informed through ongoing updates regarding the progress of the investigation, the development of the incident, identified impacts, and containment or corrective measures implemented.

Azul will investigate the causes and effects of the incident that occurred, and will then take containment measures, assess the impact, and evaluate the need to communicate the incident to the competent authority and/or the Data Subjects. For an audit of the incident to be conducted, Azul will analyze any and all information, as well as the available evidence that may identify the cause of the issue.

9. TERMINATION OF THE CONTRACT

After the termination, rescission, or expiration of the Contract, the Third Party must (i) return to Azul the Personal Data database generated or received from its activities within the scope of the Contract and, subsequently, (ii) delete such Personal Data database from its servers or other storage media, including any copies. The Third Party must prove to Azul that the Personal Data has been effectively deleted by means of a formal destruction certification, observing recognized secure disposal standards.

With respect to the Personal Data of its Collaborators, the Third Party, as sole Controller, may retain it for purposes authorized by applicable law, such as compliance with legal and regulatory obligations and defenses in legal proceedings.

10. SANCTIONS

Noncompliance with this Policy may result in the Third Party being liable for losses and damages suffered by Azul or third parties, as applicable under the Contract.

****