**DATA PROCESSING AGREEMENT**

BETWEEN:

[The data controller], a company incorporated under the laws of [country], having its registered office and principal place of business in [city] at [address] (hereinafter to be referred to as: the “**Data Controller**”),

AND

Associates for International Research, Inc. ("AIRINC"), a company incorporated under the laws of the United States, having its registered office and principal place of business in Cambridge, MA at 675 Massachusetts Avenue (hereinafter to be referred to as: the “**Data Processor**”).

HEREBY AGREE AS FOLLOWS:

1. **Subject matter of this Data Processing Agreement**
	1. This Data Processing Agreement applies exclusively to the processing of personal data that is subject to EU Data Protection Law [in the scope of the agreement of [date] between the parties for the [provision of services] (“Services”) (hereinafter to be referred to as: the “**Service Agreement**”).
	2. The term EU Data Protection Law shall mean Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, a regulation commonly known as the “General Data Protection Regulation”, as well as all local laws or regulations giving effect to GDPR in the relevant Territory, and any similar or equivalent laws.
	3. The term “GDPR” shall mean Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, a regulation commonly known as the “General Data Protection Regulation”.
	4. Terms such as “Processing”, “Personal Data”, “Data Controller” and “Processor” shall have the meaning ascribed to them in the GDPR.
	5. Insofar as the Data Processor will be processing Personal Data subject to EU Data Protection Law on behalf of the Data Controller in the course of the performance of the Service Agreement with the Data Controller the terms of this Data Protection Agreement shall apply. An overview of the categories of Personal Data, the types of Data Subjects, and purposes for which the Personal Data are being processed is provided in Annex 2.
2. **The Data Controller and the Data Processor**
	1. The Data Controller will determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by the Data Processor. The Data Processor will process the Personal Data only as set forth in Data Controller’s written instructions.
	2. The Data Processor will only process the Personal Data on documented instructions of the Data Controller in such manner as - and to the extent that - this is appropriate for the provision of the Services, except as required to comply with a legal obligation to which the Data Processor is subject. In such a case, the Data Processor shall inform the Data Controller of that legal obligation before processing, unless that law explicitly prohibits the furnishing of such information to the Data Controller. The Data Processor shall never process the Personal Data in a manner inconsistent with the Data Controller’s documented instructions. The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.
	3. The Parties have entered into a Service Agreement in order to benefit from the expertise of the Processor in securing and processing the Personal Data for the purposes set out in Annex 2. The Data Processor shall be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes, subject to the requirements of this Data Processing Agreement.
	4. Data Controller warrants that it has all necessary rights to provide the Personal Data to Data Processor for the Processing to be performed in relation to the Services. To the extent required by applicable EU Data Protection Law, Data Controller is responsible for ensuring that any necessary data subject consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. Should such a consent be revoked by the data subject, Data Controller is responsible for communicating the fact of such revocation to the Data Processor, and Data Processor remains responsible for implementing any Data Controller instruction with respect to the further processing of that Personal Data.
3. **Confidentiality**
	1. Without prejudice to any existing contractual arrangements between the Parties, the Data Processor shall treat all Personal Data as strictly confidential and it shall inform all its employees, agents and/or approved subprocessors engaged in processing the Personal Data of the confidential nature of the Personal Data. The Data Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.
4. **Security**
	1. Taking 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, without prejudice to any other security standards agreed upon by the Parties, the Data Controller and Data Processor shall implement appropriate technical and organizational measures to ensure a level of security of the processing of Personal Data appropriate to the risk. These measures shall include as appropriate:
		* + 1. measures to ensure that the Personal Data can be accessed only by authorized personnel for the purposes set forth in Annex 2 of this Data Processing Agreement;
				2. In assessing the appropriate level of security account shall be taken in particular of all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of Personal Data;
				3. the pseudonymisation and encryption of personal data;
				4. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
				5. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
				6. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Personal Data;
				7. measures to identify vulnerabilities with regard to the processing of Personal Data in systems used to provide services to the Data Controller;
				8. the measures agreed upon by the Parties in Annex 3.
	2. The Data Processor shall at all times have in place an appropriate written security policy with respect to the processing of Personal Data, outlining in any case the measures set forth in Article 4.1.
	3. At the request of the Data Controller, the Data Processor, shall demonstrate the measures it has taken pursuant to this Article 4 or Article 10.3 by answering questions asked by the Data Controller. In the event the Data Controller reasonably considers that the answers provided by Data Processor justify further analysis, Data Processor shall, in agreement with the Data Controller, either:
5. provide a statement to the Data Controller issued by a qualified independent third party assessor certifying that the Data Processor’s business processes and procedures comply with this Agreement; or,
6. shall allow the Data Controller to audit and test such measures. The Data Controller shall be entitled on giving at least 30 days’ notice to the Data Processor to carry out, or have carried out by a third party who has entered into a confidentiality agreement with the Data Processor, audits of the Data Processor´s premises and operations as these relate to the Personal Data. The Data Processor shall cooperate with such audits carried out by or on behalf of the Data Controller and shall grant the Data Controller´s auditors reasonable access to any premises and devices involved with the Processing of the Personal Data. The Data Processor shall provide the Data Controller and/or the Data Controller´s auditors with access to any information relating to the Processing of the Personal Data as may be reasonably required by the Data Controller to ascertain the Data Processor´s compliance with this Data Processing Agreement. Audits shall be conducted no more than once per year, per Client, during the term of the Agreement, during regular business hours, and shall be subject to (i) a detailed written audit plan reviewed and approved by Data Processor’s security organization; and (ii) Data Processor’s on-site security policies. Such audits will take place only in the presence of a representative of Data Processor, or such person designated by the appropriate representative. The audits shall not be permitted to disrupt Data Processor’s activities or compromise the security and confidentiality of Personal Data pertaining to other of Data Processor’s clients. Data Processor may charge Client a reasonable fee for such audit.
7. **Improvements to Security**
	1. The Parties acknowledge that security requirements are constantly changing, and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Data Processor will therefore evaluate the measures as implemented in accordance with Article 4 on an on-going basis and will tighten, supplement and improve these measures in order to maintain compliance with the requirements set out in Article 4. The Parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in applicable data protection law or by data protection authorities of competent jurisdiction.
	2. Where an amendment to the Service Agreement is necessary in order to execute a Data Controller instruction to the Data Processor to improve security measures as may be required by changes in applicable data protection law from time to time, the Parties shall negotiate an amendment to the Service Agreement in good faith.
8. **Data Transfers**
	1. The Data Processor shall immediately notify the Data Controller of any (planned) permanent or temporary transfers of Personal Data to a country outside of the European Economic Area without an adequate level of protection and shall only perform such a (planned) transfer after obtaining authorization from the Data Controller, which may be refused at its own discretion. Annex 4 provides a list of transfers for which the Data Controller grants its consent upon the conclusion of this Data Processing Agreement.
	2. To the extent that the Data Controller or the Data Processor are relying on a specific statutory mechanism to normalize international data transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the Data Controller and the Data Processor agree to cooperate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.
9. **Information Obligations and Incident Management**
	1. When the Data Processor becomes aware of an incident that impacts the Processing of the Personal Data that is the subject of the Services Agreement, it shall promptly notify the Data Controller about the incident, shall at all times cooperate with the Data Controller, and shall follow the Data Controller’s instructions with regard to such incidents, in order to enable the Data Controller to perform a thorough investigation into the incident, to formulate a correct response, and to take suitable further steps in respect of the incident.
	2. The term “incident” used in Article 7.1 shall be understood to mean in any case:
		* + 1. a complaint or a request with respect to the exercise of a data subject’s rights under EU Data Protection Law;
				2. an investigation into or seizure of the Personal Data by government officials, or a specific indication that such an investigation or seizure is imminent;
				3. any unauthorized or accidental access, processing, deletion, loss or any form of unlawful processing of the Personal Data;
				4. any breach of the security and/or confidentiality as set out in Articles 3 and 4 of this Data Processing Agreement leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data, or any significant indication of such breach having taken place or being about to take place;
				5. where, in the opinion of the Data Processor, implementing an instruction received from the Data Controller would violate applicable laws to which the Data Controller or the Data Processor are subject.
	3. The Data Processor shall at all times have in place written procedures which enable it to promptly respond to the Data Controller about an incident. Where the incident is reasonably likely to require a data breach notification by the Data Controller under applicable EU Data Protection Law, the Data Processor shall implement its written procedures in such a way that it is in a position to notify the Data Controller no later than 48 hours of having become aware of such an incident.
	4. Any notifications made to the Data Controller pursuant to this Article 7 shall be addressed to the employee of the Data Controller whose contact details are provided in Annex 1 of this Data Processing Agreement, and shall contain, to the extent known after reasonable investigation:
		* + 1. a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;
				2. the name and contact details of the Data Processor’s data protection officer or another contact point where more information can be obtained;
				3. a description of the likely consequences of the incident; and
				4. a description of the measures taken or proposed to be taken by the Data Processor to address the incident including, where appropriate, measures to mitigate its possible adverse effects.
10. **Contracting with Subprocessors**
	1. The Data Controller authorizes the Data Processor to engage the subprocessors in the country locations for the Service-related activities specified as described in Annex 2. Data Processor shall inform the Data Controller of any addition or replacement of such subprocessors giving the Data Controller an opportunity to object to such changes. Approved subprocessors are listed in Annex 5.
	2. Notwithstanding any authorization by the Data Controller within the meaning of the preceding paragraph, the Data Processor shall remain fully liable vis-à-vis the Data Controller for the performance of any such sub-processor that fails to fulfil its data protection obligations.
	3. The consent of the Data Controller pursuant to Article 8.1 shall not alter the fact that consent is required under Article 6 for the engagement of subprocessors in a country outside the European Economic Area without a suitable level of protection.
	4. The Data Processor shall ensure that the sub-processor is bound by the same data protection obligations of the Data Processor under this Data Processing Agreement, shall supervise compliance thereof, and must in particular impose on its subprocessors the obligation to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of EU Data Protection Law.
	5. The Data Controller may request that the Data Processor audit a Third Party Sub-processor or provide confirmation that such an audit has occurred (or, where available, obtain or assist customer in obtaining a third-party audit report concerning the Third Party Sub-processor’s operations) to ensure compliance with its obligations imposed by the Data Processor in conformity with this Agreement.
11. **Returning or Destruction of Personal Data**
	1. Upon termination of this Data Processing Agreement, or upon fulfillment of all purposes agreed in the context of the Services whereby no further processing is required, and upon the Data Controller’s written request, the Data Processor shall, at the discretion of the Data Controller, either delete, destroy or return all Personal Data to the Data Controller and destroy or return any existing copies.
	2. The Data Processor shall notify all third parties supporting its own processing of the Personal Data of the termination of the Data Processing Agreement and shall ensure that all such third parties shall either destroy the Personal Data or return the Personal Data to the Data Controller, at the discretion of the Data Controller.
12. **Assistance to Data Controller**
	1. The Data Processor shall assist the Data Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Data Controller’s obligation to respond to requests for exercising the data subject’s rights under EU Data Protection Law.
	2. The Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to Section 4 (Security) and prior consultations with supervisory authorities required under Article 36 of the GDPR taking into account the nature of processing and the information available to the Data Processor.
	3. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the Data Processor’s obligations and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller as described in section 4.3.
13. **Liability and Indemnity**
	1. The Data Processor indemnifies the Data Controller and holds the Data Controller harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Data Controller and arising directly or indirectly out of or in connection with a breach of this Data Processing Agreement and/or the Applicable Data Protection Law by the Data Processor. The Data Controller indemnifies the Data Processor and holds the Data Processor harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Data Processor and arising directly or indirectly out of or in connection with a breach of this Data Processing Agreement and/or the Applicable Data Law by the Data Controller.
14. **Duration and Termination**
	1. This Data Processing Agreement shall come into effect on [date].
	2. Termination or expiration of this Data Processing Agreement shall not discharge the Data Processor from its confidentiality obligations pursuant to Article 3.
	3. The Data Processor shall process Personal Data until the date of termination of the agreement, unless instructed otherwise by the Data Controller, or until such data is returned or destroyed on instruction of the Data Controller.
15. **Miscellaneous**
	1. In the event of any inconsistency between the provisions of this Data Processing Agreement and the provisions of the Service Agreement, the provisions of this Data Processing Agreement shall prevail.
	2. This Data Processing Agreement is governed by the laws of the United States. Any disputes arising from or in connection with this Data Processing Agreement shall be brought exclusively before the competent court of Massachusetts.

|  |  |  |  |
| --- | --- | --- | --- |
| Signed |  | Signed |  |
| For and on behalf of the Data Processor | For and on behalf of the Data Controller |
| Name: |  | Name: |  |
| Title: |  | Title: |  |
| Date: |  | Date: |  |

**Annex 1:**

Contact information of the data protection officer of the Data Processor.

**Gregory Lynch**

**Data Protection Officer**

**privacy@air-inc.com**

Contact information of the data protection officer of the Data Controller.

**[Contact information]**

**Annex 2:**

Personal data that will be processed in the scope of the Service Agreement and the purposes for which these data will be processed:

|  |  |  |
| --- | --- | --- |
| Category of data | Purpose of collection, processing or use of data | Categories of data subjects that are affected by the data beingprocessed  |
| Salary or job levelfamily sizelocation (country and/or city)name (optional)job title (optional)company name | Data is entered by Data Controller into allowance calculator and aggregator tools available on AIRINC’s customer web portal, AIRLinc. Only data required to fulfill the Services is processed. | Data Controller’s employees |

**Annex 3:**

Security measures:

|  |
| --- |
| See Appendix 1: Technical and Organizational Security Measures |

**Annex 4:**

Transfers to countries outside the European Economic Area without a suitable level of protection for which the Data Controller has granted its authorization:

|  |
| --- |
| Data processing countries |
| AIRINC’s main data center is located in the Boston, MA, United States, most data is processed and stored at this location. Transfer to this location is governed by AIRINC’s registration in the EU-US Privacy Shield Framework. |

**Annex 5:**

Approved subprocessors:

|  |  |
| --- | --- |
| Subcontractor name and address | Activities to be carried out |
| NetSuite | Accounting and invoicing |
| MaritzCX Research LLC | Customer policy and practice surveys |
| Mimecast | Email security and GDPR compliance |
|  |  |

# Appendix 1

# Technical and Organizational Security Measures

# Physical Access Control

|  |
| --- |
| Control |
| Security perimeters are defined and used to protect areas that contain personal data and processing facilities. |
| Secure areas are protected by appropriate entry controls. Only authorized personnel are allowed access. A visitor and supplier access rule is in place. |
| Physical security for offices, rooms, and facilities is designed and applied. |
| Procedures for working in secure areas are designed and applied. |
| Access points such as delivery and loading areas, and other points where unauthorized persons could enter the premises, are controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. |

#

# Logical Access Control

## General Access Control and Authentication

|  |
| --- |
| Control |
| An access control policy is established, documented and regularly reviewed based on business and information security requirements. |
| The allocation of secret authentication information is controlled through a formal management process. |
| Users are required to adhere to their responsibilities regarding use of secret authentication information. |
| Where required by the access control policy, access to systems and applications is controlled by a secure log-on procedure. |
| Password management systems are interactive and shall ensure quality passwords. |
| A policy and supporting security measures is adopted to manage the risks introduced by using mobile devices. |
| A policy and supporting security measures is implemented to protect information accessed, processed, or stored at teleworking sites. |
| Users ensure that unattended equipment has appropriate protection. |
| A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities is adopted. |

##

## Network Security

|  |
| --- |
| Control |
| Users are only provided with access to the network and network services that they have been specifically authorized to use. |
| Networks are managed and controlled to protect information systems and applications. |
| Security mechanisms, service levels, and management requirements of all network services are identified and included in network services agreements, whether these services are provided in-house or outsourced. |
| Groups of information services, users, and information systems are segregated on networks. |

## Secure System Development

|  |
| --- |
| Control |
| The information-security related requirements are included in the requirements for new information systems or enhancements to existing information systems. |
| Rules for the development of software and systems are established and applied to developments within AIRINC. |
| Access to program source code is restricted. |
| Principles for engineering secure systems are established, documented, maintained, and applied to any information system implementation efforts. |
| AIRINC established and appropriately protects secure development environments for system development and integration efforts that cover the entire system development lifecycle. |
| AIRINC does not outsource any development of software or systems. |

## Logging and Log Management

|  |
| --- |
| Control |
| Event logs recording user activities, exceptions, faults, and information security events are produced, kept, and regularly reviewed. |
| Logging facilities and log information are protected against tampering and unauthorized access. |
| System administrator and system operator activities are logged and the logs protected and regularly reviewed. |
| A consistent time synchronization ensures proper time-wise logging on all servers, firewalls, routers and further network devices. |

## Technical Vulnerability Management and Protection from Malware

|  |
| --- |
| Control |
| Detection, prevention, and recovery controls to protect against malware are implemented, combined with appropriate user awareness. |
| Information about technical vulnerabilities of information systems is being obtained in a timely fashion, AIRINC’s exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. |

# Data Access Control

## Authorization

|  |
| --- |
| Control |
| A formal user registration and de-registration process is implemented to enable assignment of access rights. |
| A formal user access provisioning process is implemented to assign or revoke access rights for all user types to all systems and services. |
| User access is provisioned based on the least privilege principle.  |
| The allocation and use of privileged access rights is restricted and controlled. |
| Asset owners review users’ access rights at regular intervals. |
| The access rights of all employees and external party users to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change. |
| Information involved in web application service transactions is protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, or replay. |

## Use of Cryptography

|  |
| --- |
| Control |
| A policy on the use of cryptographic controls for protection of information shall be developed and implemented. |
| A policy for the use, protection and lifetime of cryptographic keys is defined and implemented. |
| All items of equipment containing storage media are verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. |

##

## Asset Management and Information Classification

|  |
| --- |
| Control |
| Assets associated with information and information processing facilities are identified and an inventory of these assets is drawn up and maintained. |
| Assets maintained in the inventory are owned. |
| Rules for the acceptable use of information and of assets associated with information and information processing facilities are identified, documented, and implemented. |
| All employees receive data privacy and protection training upon hire and annually. |
| All employees and external party users return all AIRINC-owned assets in their possession upon termination of their employment, contract or agreement. |
| Information is classified in terms of legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification. |
| Procedures for handling assets are developed and implemented in accordance with the information classification scheme adopted by AIRINC. |
| Procedures are implemented for the management of removable media in accordance with the classification scheme adopted by AIRINC. |
| Media is disposed of securely when no longer required, using formal procedures. Where hardcopy materials are destroyed, they are destroyed securely using mechanisms such as cross-cut shredding. |

# Data Transfer Control

|  |
| --- |
| Control |
| Individuals under AIRINC’s control with access to Personal Data are subject to a confidentiality obligation. |
| Portable devices containing information are protected against unauthorized access, misuse, or corruption during transportation. |
| Formal transfer policies, procedures, and controls are in place to protect the transfer of information through the use of all types of communication facilities. |
| Agreements address the secure transfer of business information between AIRINC and external parties. |
| Information involved in electronic messaging is appropriately protected. |
| Requirements for confidentiality or non-disclosure agreements reflecting AIRINC’s needs for the protection of information are identified, regularly reviewed, and documented. |

# Input Control

|  |
| --- |
| Control |
| All critical devices, systems, databases and applications must have logging enabled to capture sufficient information to establish a proper verifiability of occurring events. |
| Log information is protected against unauthorized access. |
| Access to systems, applications and the regarding data is always based on individual, personally associated user identifiers. |
| The use of privileged utility software is consistently logged. |

# Availability Control

## Backup

|  |
| --- |
| Control |
| Backup copies of information, software, and system images are taken and tested regularly in accordance with an agreed backup policy. Recovery tests are performed on a periodic basis. |
| Records are protected from loss, destruction, falsification, unauthorized access, and unauthorized release in accordance with legal, regulatory, contractual, and business requirements. |

## Change Control

|  |
| --- |
| Control |
| Documented operating procedures are made available to all users who need them. |
| Changes to systems within the development lifecycle are controlled by the use of change control procedures. |
| When operating platforms are changed, business critical applications are reviewed and tested to ensure there is no adverse impact on operations or security. |
| Modifications to software packages are limited to necessary changes, and all changes shall be strictly controlled. |
| Testing of security functionality is carried out during development. |
| Acceptance testing programs and related criteria is established for new information systems, upgrades, and new versions. |
| Rules governing the installation of software by users are established and implemented. |

## Business Continuity and Disaster Recovery

|  |
| --- |
| Control |
| AIRINC determines its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster. Processes and controls are established, documented, implemented, maintained and verified to ensure the required level of continuity for information security during an adverse situation. |
| Information processing facilities are implemented with redundancy sufficient to meet availability requirements. |

##

## Operational Aspects

|  |
| --- |
| Control |
| The use of resources is monitored, tuned and projections made of future capacity requirements to ensure the required system performance. |
| The clocks of all relevant information processing systems within a security domain are synchronized to a single reference time source. |
| Requirements and activities involving verification of operational systems are planned and agreed to minimize disruptions to business processes. |
| Equipment is sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. |
| Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference, or damage. |

# Data Separation

|  |
| --- |
| Control |
| Access to information and application system functions is restricted in accordance with the access control policy. This includes the appropriate isolation of Personal Data. |
| Development, testing, and operational environments are separated to reduce the risks of unauthorized access or changes to the operational environment. |
| Test data is selected carefully, protected, and controlled. Personal Data is not utilized for testing purposes during the software development lifecycle. |