**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 Schedule 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 Massachusetts, United States, most data is processed and stored at this location.  |

**Annex 5:**

Approved subprocessors:

|  |  |
| --- | --- |
| Subcontractor name and address | Activities to be carried out |
| NetSuite1900 Market Street, 8th FloorPhiladelphia, PA 19103 United States | Accounting and invoicing |
| MaritzCX Research LLC1111 Olive Street, St. Louis, MO 63101 United States | Customer policy and practice surveys |
| Mimecast191 Spring Street, Lexington, MA 02421 United States | Email security and GDPR compliance |
| HubSpot25 First St., 2nd floor, Cambridge, MA 02141 United States | Marketing and news communications |

# Schedule 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. |

Schedule 2

Standard Contractual Clauses (processors)

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

Name of the data exporting organisation:

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

……………………………………………………………
(the data **exporter**)

And

Name of the data importing organisation:

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

…………………………………………………………………
(the data **importer**)

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 Appendix 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[[1]](#footnote-1);

(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[[2]](#footnote-2)**

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:

(i) 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,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) 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;

(f) 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;

(g) 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;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) 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 of 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 it 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[[3]](#footnote-3). Where the subprocessor fails to fulfil 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 notified 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.

**On behalf of the data exporter:**

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

 (stamp of organisation)

**On behalf of the data importer:**

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

 (stamp of organisation)

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

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 (please specify briefly your activities relevant to the transfer):

………………………………………………………………………………………………………………………………………………………………………………………………

**Data importer**

The data importer is (please specify briefly activities relevant to the transfer):

………………………………………………………………………………………………………………………………………………………………………………………………

**Data subjects**

The personal data transferred concern the following categories of data subjects (please specify):

………………………………………………………………………………………………………………………………………………………………………………………………

**Categories of data**

The personal data transferred concern the following categories of data (please specify):

………………………………………………………………………………………………………………………………………………………………………………………………

**Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data (please specify):

………………………………………………………………………………………………………………………………………………………………………………………………

**Processing operations**

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

………………………………………………………………………………………………………………………………………………………………………………………………

DATA EXPORTER

Name:………………………………

Authorised Signature ……………………

DATA IMPORTER

Name:………………………………

Authorised Signature ……………………

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

……………………………………………………………………………………………………………………………………………See Schedule 1 Technical and Organizational Security Measures ……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

1. Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the **contract** to stand alone. [↑](#footnote-ref-1)
2. Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter* *alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements. [↑](#footnote-ref-2)
3. This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision. [↑](#footnote-ref-3)