DATA PROCESSING AGREEMENT

THIS DATA PROCESSING AGREEMENT (HEREINAFTER "DPA") IS BETWEEN ARKADIN AND CLIENT AND SHALL TAKE EFFECT AND BECOME BINDING BETWEEN ARKADIN AND CLIENT TO THE EXTENT THAT ARKADIN PROCESSES CLIENT'S PERSONAL DATA FOR WHICH CLIENT IS DATA CONTROLLER, AND, WHERE A DPA IS REQUIRED UNDER THE APPLICABLE DATA PROTECTION LEGISLATION. FOR THE AVOIDANCE OF ANY DOUBT, THIS DPA SHALL NOT BE BINDING WHERE THE ENTITY SIGNING THIS DPA IS NOT A PARTY TO ARKADIN CONTRACT.
THIS DPA AND THE EUROPEAN COMMISSION STANDARD CONTRACTUAL CLAUSES HAVE BEEN PRE-SIGNED BY ARKADIN REPRESENTATIVE. CLIENT MUST COMPLETE AND SIGN THE DPA PAGES 6 (ARTICLE 12.2 AND SIGNATURE PAGE) AND 11 AND SUBMIT THE FULLY SIGNED COPY BY EMAIL TO DPA@ARKADIN.COM INDICATING CLIENT NAME. ONCE ARKADIN WILL RECEIVE THE COMPLETED AND SIGNED COPY BY CLIENT, THIS DPA WILL BECOME A LEGALLY BINDING ADDENDUM TO ARKADIN CONTRACT.

1. BACKGROUND

Arkadin has entered into contract with the Client to provide services involving the processing of Client Personal Data (hereinafter the "Contract"). This DPA shall apply to all processing of Client's Personal Data by Arkadin in order to provide the services under the Contract(s).

The Client and Arkadin enter into this DPA on their behalf and, to the extent required under applicable Data Protection Law and Regulation as defined below, in the name and on behalf of their respective Affiliates, if and to the extent (i) Arkadin processes Personal Data for such Affiliates, and (ii) to the extent the Client controls Personal Data of such Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the term (i) "Client" shall include the Client and its Affiliates; (ii) "Arkadin" shall include Arkadin and its Affiliates.

The DPA is an addendum to and forms part of the Contract.

For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows.

2. DEFINITION

The terms which follow shall have the following meanings:

"**Affiliate**" refers to, now or in the future, any other entity that (i) directly controls[1]; (ii) is under common control with; or (iii) is controlled by Arkadin or the Client, respectively. An entity shall be considered as controlling another entity if it owns or controls at least fifty (50) percent of the voting stock or other ownership interest of the other entity.

"**Arkadin**" means the Arkadin entity which is a party to the Contract with the Client and that shall be deemed the Data Processor for purposes of this DPA.

"**Client**" means the entity which is a party to the Contract and that shall be deemed the Data Controller for purposes of this DPA.

[1] The foregoing shall not apply to Arkadin SAS

"**Data Controller**" means the natural or legal personal, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

"**Data Processor**" means the natural or legal personal, public authority, agency or any other body which processes personal data on behalf of the Data Controller.

"**Data Protection Law and Regulation**" means the Regulation (EU) 2016/679 of the European parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, the General Data Protection Regulation (or "**GDPR**") and laws implementing or supplementing such GDPR.

"Personal Data" means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an onine identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Standard Contractual Clauses" means the agreement executed by and between Client and Arkadin and attached hereto as Schedule 3 pursuant to the European Commission's decision (C(2010)593) of February 5, 2010 on Standard Contractual Clauses for the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of data protection.

"Sub-processor" means any person or entity (including any third party and any Arkadin's Affiliate) appointed by or on behalf of Arkadin who may process Personal Data.

Arkadin and the Client are hereinafter individually designated as a "**Party**" and collectively as the "**Parties**".

Terms used in this DPA other than those defined above shall have the meaning ascribed to them in the GDPR.

All capitalised terms not otherwise defined herein shall have the meaning set forth in the Contract.

For the avoidance of doubt, unless there is any conflict or inconsistency between the provisions relating to processing of Personal Data in the Contract and this DPA (in which case the provisions of this DPA take precedence), all other provisions of the Contract shall continue to apply.

3. STATUS OF THE PARTIES

3.1. Each Party undertakes to comply with its obligations regarding the Data Protection Law and Regulation. The Parties have agreed that the Client is the Data Controller and Arkadin is the Data Processor of the Personal Data collected in the European Economic Area ("EEA") and Switzerland, provided directly or indirectly to Arkadin by the Client and the Moderators who have been granted access to the Services by the Client.

3.2. As Data Controller, the Client shall have sole responsibility for the accuracy, reliability and suitability of the Personal Data. The Client shall be responsible for making all the necessary declarations. The Client undertakes to indemnify and hold Arkadin, its representatives, employees, and Sub-processors harmless in respect of all claims, liabilities, damage, and expenses (including legal costs, fees and expenses) imposed on or incurred by Arkadin, its representatives, employees, and Sub-processors arising from any failure to respect this obligation.

3.3. As Data Processor, Arkadin undertakes to process the Client Personal Data pursuant to the Client's instructions and/or as is strictly necessary for the performance of the Services.

In this respect, Arkadin undertakes to:

- refrain from processing the Client Personal Data for purposes other than performance of the Services;
- take all appropriate and relevant measures to abide by the legal and regulatory provisions regarding Personal Data protection;
- observe the data retention period applicable to the purposes for which they have been collected or supplied, and delete/archive or anonymise them once the purpose no longer exists, subject to legal requirements;
- notify any Client Personal Data breach pursuant to Articles 33 and 34 of the GDPR. Arkadin will co-operate with the Client and take such reasonable steps as are agreed in good faith by the Parties to assist in the investigation, mitigation and remediation of each Personal Data breach. To the extent that the Client is responsible for a Personal Data breach, the Client will reimburse Arkadin for all documented costs reasonably and properly incurred by Arkadin performing its obligations under this paragraph (including internal costs and third-party costs including legal fees);
- ensure that the persons authorised to process the Personal Data undertake to protect the confidentiality thereof;
- contribute to audits conducted by the Client and provide it with all the information required to demonstrate compliance with the obligations laid down in the article 28-3 of the GDPR, subject to the conditions of the article 10 below.

4. RIGHTS OF DATA SUBJECTS

The Parties undertake to observe Data Subjects' rights to access, rectify, object to, erase, and restrict Personal Data processing and Personal Data portability as detailed in Chapter 3 of the GDPR. If a Data Subject contacts Arkadin directly to exercise any of its rights in respect of its Personal Data, Arkadin undertakes to inform the Client of this request immediately and to cooperate with the Client as reasonably requested to enable it to comply with its obligations. Arkadin shall respond to these requests only on the written instruction of the Client to this end.

5. ARKADIN PERSONNEL

Arkadin will take reasonable steps to ensure the reliability of any of its employees, agents or contractors who may have access to Client Personal Data, ensuring that such individuals are subject to confidentiality obligations or professional or statutory obligations of confidentiality.

6. SUBPROCESSING

6.1. By signing the DPA, the Client grants Arkadin a general written authorisation to engage, as reasonably necessary for the provision of the services, the Sub-processors listed on the following page: https://www.arkadin.com/en-gb/data-subprocessors Arkadin provides its Clients with a mechanism to subscribe to update notifications directly on this page.
According to this general authorisation, Arkadin undertakes to inform any subscriber of any intended changes subject to a thirty (30) day-prior written notice concerning the addition or replacement of Sub-processors, thus providing the Client with an opportunity to raise any objections it may have to these changes. If the Client has legitimate and reasonable reasons to object the appointment of a new Sub-processor occurring after the date of signature of the DPA, the Client shall immediately supply grounds for this objection to Arkadin by sending written notice to Arkadin at privacy@arkadin.com, within thirty (30)

business days of the Arkadin's notice, failing which the Client shall be deemed to have approved and agreed to such appointment.

6.2. If Arkadin is unable to avoid the Personal Data being processed by the new Sub-processor, the Client shall have the right, within thirty (30) days of the notification, to terminate that part of the Contract affected by the update in question.

6.3. With respect to each Sub-processor, Arkadin will: (a) exercise commercially reasonable care in the assessment, appointment and oversight of the relevant processing activities of Sub-processors; (b) include terms in the contract between Arkadin and each Sub-processor which offer an equivalent level of protection for client Personal Data as those set out in this DPA; and (c) remain fully liable to the Client for any failure by each Sub-processor to fulfil its obligations in relation to the processing of Client Personal Data.

7. TRANSFERS OF CLIENT PERSONAL DATA

7.1. Arkadin hereby informs the Client that the Personal Data may, solely as required for the performance of the Services ordered, be transferred by Arkadin to third countries, to Sub-processors as listed here.

7.2. Arkadin enters in the name and on behalf of its Affiliates located within third countries and listed in the Schedule 1 into the Standard Contractual Clauses attached hereto as Schedule 3 with the Client. These Standard Contractual Clauses will apply with respect to any Personal Data originating within the EEA and Switzerland which will be transferred by Arkadin to any Affiliates of Arkadin as Sub-processor(s) located within third countries.

7.3. Regarding any other Sub-processors listed in the article 6.1, if the arrangement involves a transfer to a third country which legislation has not been recognised as offering an adequate level of protection to Personal Data, Arkadin ensures that adequate contractual measures are in place as required by Data Protection Law and Regulation, and where the Personal Data is from the EEA or Switzerland, the Standard Contractual Clauses or equivalent ad hoc clauses are incorporated into the contract between Arkadin and the Sub-processor.

8. DISCLOSURE OF PERSONAL DATA

Arkadin undertakes not to disclose the Personal Data to any third party, except (i) at the request of the Client, (ii) pursuant to the provisions of the Contract, or (iii) if required to do so by law.
In the event of a third party contacting Arkadin with a view to obtaining certain Personal Data, Arkadin shall invite the third party to make its request directly to the Client. If Arkadin is obliged by law to disclose Personal Data to the authorities, it undertakes to inform the Client accordingly without undue delay and supply a copy of the request, unless this is prohibited by law.

9. SECURITY

In respect to the Services, Arkadin implements appropriate technical and organisational security measures that comply with applicable Data Protection Law and Regulation and are designed to ensure a level of security appropriate to the risks that are presented by the processing of Client's Personal Data, as set forth in Schedule 2 (Technical and Organisational Measures). In assessing the appropriate level of security, Arkadin will take into account the risks that might result from accidental or unlawful destruction or corruption, loss, alteration, unauthorised disclosure of, or access to, Personal Data it may transmit, store or otherwise process, pursuant to Article 32 of the GDPR.

10. AUDIT

The Client shall, subject to a notice period of not less than fifteen (15) calendar days, inform Arkadin in writing of its intention to conduct an audit to monitor Arkadin's obligations according to the DPA. The audits may not occur more than once per contractual year and shall be undertaken during normal business days and hours of Arkadin.

The Client and Arkadin shall each appoint a coordinator who shall be responsible for preparing and monitoring the audits. Coordinators shall mutually agree, acting in good faith, to the purpose of the audit, its objectives, schedule, and the number, the premises concerned, the qualification and identity of the auditors. The audit shall be limited to the monitoring of processes, organisation and tools directly and exclusively related to the GDPR provisions.

All documents and information required for the performance of the audit shall be made available to auditors by Arkadin exclusively on the premises of the latter, without the possibility of being removed or of being copied, for any purposes whatsoever. This shall additionally be applicable to documents and information made available by Sub-processors of Arkadin.

Any auditor appointed by the Client shall be approved by Arkadin and shall sign a confidentiality agreement with Arkadin, which may include the obligation not to communicate to the Client any confidential information made available to the auditor during the audit, with the exception of that information related to any failure of Arkadin to comply with the article 28-3 of the GDPR.

In no case shall the audit have the purpose of monitoring or requiring access to:

- any non-specific Personal Data of the Client, whether confidential or not, or information which disclosure may, to Arkadin's discretion, adversely affect the security of Arkadin sites or of other of its clients;
- Arkadin's financial data;
- personal Data pertaining to Arkadin or Arkadin's Sub-processor employees.

As the case may be, should the audit require additional internal or external resources (including resources of Arkadin's Sub-processors) to the resources reasonably required under similar circumstances or as agreed by the coordinators as stated above, Arkadin may invoice such resources to the Client, at the then current rates applicable to professional services.

Any information collected shall not be used for any other purposes than the concerned audit.

It is hereby agreed that all activities undertaken within the framework of an audit shall not, whether concurrently or otherwise: (i) be likely to hinder, modify or otherwise adversely affect the operation of any services, systems, networks, software and/or hardware other than those allocated for exclusive use of the Client; (ii) harm, delete, modify any data other than those of the Client; (iii) enable unauthorised access to or maintenance of aforementioned data.

No intruder or penetration tests into the Arkadin network shall be permitted for whatsoever reasons and shall be excluded from the audits.

The auditor shall notify in writing the audit report to Arkadin. Should the audit report evidence any Arkadin's material failure to comply with its obligations according to the DPA, Arkadin shall be entitled to remedy such failure, within one (1) month from the notification of the audit report to Arkadin, and to propose to the Client an action plan incorporating remedial measures and the calendar associated thereto.

11. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Upon Client's request and subject to the nature of the relevant processing by and information available to Arkadin, Arkadin will provide reasonable assistance to the Client with any data protection impact assessments and any prior consultations to any supervisory authority of the Client, which are required under applicable Data Protection Law and Regulation. The Client will reimburse Arkadin in full for all documented costs reasonably incurred by Arkadin in performing its obligations under this article (including internal costs and third-party costs including legal fees).

12. CONTACT

12.1 - Arkadin privacy contact:
In the event of questions about the Personal Data processing performed by Arkadin pursuant to the Contract, the Client may contact Arkadin's Compliance department at: privacy@arkadin.com
Arkadin SAS is Arkadin's data protection representative within the European Economic Area and Switzerland. The lead authority is CNIL (https://www.cnil.fr). Arkadin SAS data protection officer may be contacted at the following address: Arkadin SAS – Data Protection Officer – 32 rue Guersant, 75017 Paris, France.

12.2 - Client privacy contact:
Please insert Client privacy dedicated e-mail address: _____

The DPA shall automatically terminate contemporaneously with the termination or expiry of the Contract.

13. GOVERNING LAW

The DPA shall be governed by and construed in accordance with the national law that applies to the Data Controller.

14. EFFECTIVE DATE

This Data Protection Agreement shall enter into force upon its signature.

SCHEDULES:

1/Details of processing of Client Personal Data
2/Technical and organisational measures
3/Standard Contractual Clauses (Processors)

For and on behalf of Arkadin	**For and on behalf of the Client**
Date: 20th February 2019	Date: _____
Name: Didier Jaubert	Name: _____
Title: CEO	Title: _____
Signature:	Signature:

SCHEDULE 1: DETAILS OF PROCESSING OF CLIENT PERSONAL DATA

This Schedule 1 includes certain details of the processing of Client Personal Data as required by Article 28(3) GDPR.

Data Controller and data exporter: the data controller and data exporter is the Client as mentioned in the Contract signed with Arkadin

The Data Controller's activities involve the use of collaboration services (audio, video, web conferencing, digital engagement (event and Webcast) and/or unified communications services) by the Data Subjects described below.

Data Processor(s):
Arkadin SAS and its Affiliates
The Data Processor´s activities include account management and/or support and maintenance for the provision to the Data Subjects of the collaboration services (audio, video, web conferencing, event and Webcast, and/or unified communications services).

Data importers (Arkadin signs the Standard Contractual Clauses in the name and on behalf of the following data importers):
Arkadin Australia PTY Ltd., Arkadin do Brasil Serviços de Conferencia Ltda., Arkadin GCT Technology Co. Ltd., Arkadin Colombia SAS, GCT Telecommunication (HK) Ltd., Arkadin (HK) Ltd., Arkadin Conferindia Pvt. Ltd., Arkadin Japan Co., Ltd. Arkadin Korea Ltd., Arkadin (Malaysia) SDN. BHD., Arkadin Mexico SA de CV, Arkadin Rus OOO, Arkadin (Singapore) Pte. Ltd., Arkadin South Africa (Pty) Ltd., Arkadin Global Telekonferans Hizmetleri Limited Sirketi, Arkadin Middle East FZ-LLC, Arkadin, Inc.

Data Subjects:
- Employees or contact persons of Client;
- Agents, advisors, freelancers of Client (who are natural persons);
- Client's user authorized by Client to use the services;
- All attendees designated by the Data Controller/data exporter to attend an audio, video, web, event and/or unified communications conference call thereby accessing collaboration services mentioned above.

Categories of Personal Data processed:
Registration information
- Civil status and identity (surname, first name, title, position)
- Professional contact details (email, address, phone number)
- Economic and financial information (banking data)

Host and usage information
- Connection data (IP address, logs, identifiers, moderator pin code, participant pin code, web login time stamp information)
- Telephony data (CDR)

User generated information (message, chats, conversations)

Special categories of data (if appropriate):
None

Processing:
Arkadin services involve the collection, recording, organisation, storage, retrieval, consultation and use, disclosure by transmission and erasure Client's personal data.

Processing Purposes:

- Performance of the services and account management: provide Client with users account (account set up and management for users), process orders, provide technical support, maintenance and resolution of users enquiries, consulting, storage, hosting and other services delivered to the Client and its users;
- Fulfill other obligations mentioned under the Service Order Form;
- Administrate contractual relationship;
- Invoicing and collection purposes;
- Improve Arkadin offerings;
- Marketing activities and web analytics as permissible under applicable law;
- Reporting;
- Security, fraud detection and prevention;
- Compliance with law and regulation.

SCHEDULE 2: TECHNICAL AND ORGANISATIONAL MEASURES

1. **Access Control to Processing Areas**. Data importer implements suitable measures in order to prevent unauthorised persons from gaining physical access to the data processing equipment where the Personal Data are processed or used. This is accomplished by :

- The equipment on which the Personal Data is processed is placed within a physically protected site secured against accidents, hazards such as fire and flooding, attacks and physical access by unauthorised and/or uncontrolled individual.
- Access authorisations are established for staff and third parties to this site. The list of entitled individuals is reviewed periodically to reflect fluctuations and changes in roles and responsibility.
- This access to the site is under control of specific management.
- Access to the site is established only to the identified group of people needed to support the required service level.
- Secured doors are in place to access the physical site.
- In addition the site access is supervised and secured by an appropriate security system and/or security organisation using a video control system.
- The physical site is only entered when work requiring access on site has to be done.

2. **Access Control to Data Processing Systems**. Data importer implements suitable measures to prevent its data processing systems from being used or logically accessed by unauthorised persons. This is accomplished by :

- User Identification and user authentication methods to grant access to the processing system are in place. Individual authentication credentials such as user IDs or similar are used that, once assigned, cannot be re-assigned to another person.
- Access control and authorisations are defined according to a 'need to have' principle and are implemented in such a way that users are uniquely identified and approved by business owners. A deactivation of user authentication credentials in case he is disqualified from accessing the date, except for those accounts authorised solely for technical management.
- Privileged accounts are reserved for specific functions and not used outside of the required need of usage. System administrators are identified and named and an up to date list with area covered is provided if requested.
- Access control mechanisms as password rules, lockouts or automatic timeouts are in place in accordance with defined overall standards.
- Internet or end user facing endpoints are protected to present unwanted access to the systems and to avoid infiltration of malicious software. This covers areas as firewalls, antivirus, detection, malware detection, and others and is adjusted to new technologies based on the overall development.

3. **Access Control to Use Specific Areas of Data Processing Systems**. Data importer commits that the persons entitled to use its data processing system are only able to access the data within the scope and to the extent covered by its access permission (authorisation) and that Personal Data cannot be read, copied or modified or removed without authorisation. This shall be accomplished by :

- Policies related to the access to Personal Data are in place and trained. To ensure that staff will only access Personal Data and resources required to perform their job duties, staff are informed about their obligation and the consequences of any violations of such obligation.
- Standard access, alteration and deletion logging is done with the base methods available on the OS, BD, Network and application areas. Enhanced logging can be done on request and with special efforts based on the available functionalities of the of the implemented technologies and applications.

4. **Transmission Control**. Data importer implements suitable measures to prevent the Personal Data from being read, copied, altered or deleted by unauthorised parties during the transmission thereof during the transport of the data media. This is accomplished by :

- Network and network access protection technologies are used.

- Monitoring of the completeness and correctness of the transfer of data is supported by using networking protocols (TCP) with error correction features.

5. **Input Control**. Data importer implements suitable measures to ensure that it is possible to check and establish whether and by whom Personal Data have been input into data processing systems or removed. This is accomplished by :

- An authorisation policy for the input of data, as well as for the reading, alteration and deletion of stored data is in place as described in section 'Access Control to Data Processing Systems'.
- If required for an adequate protection the data importer activates application functionalities to log automatically user information when data is created, modified or deleted.

6. **Job Control**. Data importer ensures that Personal Data may only be processed for the purpose described in Schedule 1 herein. This is accomplished by :

- Supporting functions executing tasks / jobs are identified and named.
- Access granted to supporting functions executing tasks / jobs is in accordance with the defined instructions.

7. **Availability Control**. Data importer implements suitable measures to ensure that Personal Data are protected from accidental destruction or loss. This is accomplished by :

- Availability is managed and designed based on an overall service level concept.
- The physical site where the data processing equipment is located is protected against general environmental hazard and unauthorised access. It is protected with specific measures against power loss thought UPS and Diesel engines. It monitors and controls temperature and humidity at the site and alerts where reaching limits.
- Availability of the network access to the site is enhanced thought WAN based redundancies, network access redundancies to the site.
- Redundancies of the infrastructure components itself (servers and storage arrays) are in place in accordance with the agreed and predefined service levels.
- The redundancy measures are check on a regular base. The results are documented accordingly.
- Functionalities are used on DB level to target for a minimum loss of transaction information in case of a technical failure. This is done by using DB features supporting minimal loss of transaction information were possible and meaningful.
- In line with the service levels defined additional availability features on DB level (real application clustering) or at application level (application based replication, load balancing) are in place.
- To reduce unscheduled downtimes proactive infrastructure maintenance is done. This maintenance work is planned and based on a predefined schedule. During these maintenance windows proactive tasks are executed to keep the infrastructure on a supported level aligned with the providers of the infrastructure components.
- After serious events a structured After Action Review is executed to detect mitigation actions and potential proactive measures.
- Technical and application related changes follow change management processes, supported where possible by multiple tiers where changes are applied first before being applied to the production environment.

8. **General Controls**. Data importer will in addition apply the following procedures:

- Regular checks of the herein described measures are scheduled and executed.
- To detect security or data integrity related threats, to investigate violation of privacy issues or other malicious attacks the data importer may use enhanced monitoring and surveillance techniques to detect any misuse of threatening behavior without disclosing this beforehand.

SCHEDULE 3: STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

The Standard Contractual Clauses are available at the following link: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32010D0087. By reference to this link , the parties hereby agree that the Standard Contractual Clauses shall be deemed incorporated into this DPA.

On behalf of each data importer:

ARKADIN

Name: Didier Jaubert

Position: CEO

In its capacity on behalf and in the name of each further data importer specified in Schedule 1.

Signature:

On behalf of the data exporter:

Name of the legal entity:_____

Name (written out in full): _____

Position: _____

Signature:_____