APPENDIX B – DATA PROCESSING TERMS OF SERVICES

The purpose of this DPA is to reflect the parties' agreement with regard to the processing of Personal Data in accordance with the requirements of Data Protection Regulations.

In respect of the processing of Personal Data of the Customer by Cloud-IAM under the Terms of Services, the parties acknowledge that the Customer is the Data Controller and Cloud-IAM is the Data Processor and both agree to comply with all corresponding obligations as per the Data Protection Regulations.

The Customer gives instructions to Cloud-IAM to process such Personal Data on its behalf as it is necessary for the purposes of the Terms of Services as defined in Appendix 1 "Description of Personal Data processing". The Appendix 1 is filled out by the Customer and shall be updated if any change is made by the Customer.

ARTICLE 1. COMPLIANCE WITH DATA PROTECTION REGULATIONS

Each party shall comply with its obligations under the Data Protection Regulations.

All capitalized words in the DPA shall have the meaning ascribed to them in the GDPR, the Data Protection Regulations and in the Terms of Services.

ARTICLE 2. DATA PROCESSING OPERATIONS UNDER THE DPA

As a reminder, for every processing carried out under this DPA, the Customer shall:

- Document the instructions related to Personal Data,
- Provide the information related to the processing to fill the Appendix 1 by contacting Cloud-IAM via the support email address: support@cloud-iam.com.

The Customer warrants to Cloud-IAM that it is entitled to transfer the Personal Data to the Cloud-IAM and/or the Sub-processor(s) in full compliance with Data Protection Regulations, including as needed, compliance to any prior required formalities and Data Subject rights, such as information and/or consent when such is required under Data Protection Regulations.

The Customer acknowledges that it is and shall remain solely responsible for determining the purposes and the means of Cloud-IAM's processing the Personal Data. The Data Controller remains solely responsible for the accuracy and adequacy of the aforementioned instructions. Any changes to the instructions given or the security measures that are required by the Customer, including in order to comply with applicable data protection laws, shall be agreed by the parties and/or via an amendment to this DPA. Any costs incurred by Cloud-IAM in complying with such changes shall be borne by the Customer.

The Customer undertakes that the Data Subjects have been informed or will be informed before the transfer of their Personal Data to Cloud-IAM in the scope of the Services.

The Product is not intended to process Special Categories of Personal Data. Therefore, the Customer undertakes to prevent any processing of Special Categories of Personal Data through the Product and the Services. However, at the Customer request, processing of Special Categories of Personal Data may be performed by Cloud-IAM. In such case, the Processing shall be covered by a specific addendum to the DPA to be entered into between the Customer and Cloud-IAM.

In case the Customer expressly requests the assistance of Cloud-IAM for the fulfilment of its obligation under the Data Protection Regulations, then Cloud-IAM shall address to the Customer the estimated costs for such assistance. Upon express acceptation of the estimated cost, Cloud-IAM shall provide assistance pursuant to the instructions of the Customer and the terms of the present DPA.

ARTICLE 3. SCOPE & INSTRUCTIONS

Cloud-IAM undertakes to:

a) solely process the Customer's Personal Data disclosed by the Customer as well as those collected or produced during the Terms of Services for the purpose(s) fulfilling its obligations under the Terms of Services and in compliance under the Customer's documented instructions, unless otherwise required by applicable Data Protection Regulations;
b) ensure that any person acting under its authority, who has access to the Customer's Personal Data disclosed by the Customer as well as those collected or produced during the Terms of Services, will process those data solely for the purpose of fulfilling Cloud-IAM's obligations under this Terms of Services and on instructions from the Customer, unless required by applicable Data Protection Regulations;
c) refrain from using Customer's Personal Data for any misappropriated, fraudulent or personal use, including for commercial purposes;
d) immediately inform the Customer if, in its opinion, a Customer's instruction infringes applicable Data Protection Regulations.

ARTICLE 4. COMMUNICATION OF CUSTOMER'S PERSONAL DATA TO THIRD PARTIES

The Customer's Personal Data processed under the DPA shall not be subject to any assignment, lease, concession, communication or disclosure to a third party, including sub-Processors of Cloud-IAM, except otherwise required by the Terms of Services or by a legal or regulatory mandatory provision.

In such a case, Cloud-IAM shall inform the Customer of that legal requirement before Processing, unless that legal or regulatory mandatory provision prohibits such information on important grounds of public interest.

ARTICLE 5. SUB-PROCESSING

With respect to the conditions referred to in paragraphs 2 and 4 of article 28 of GDPR for engaging another Data Processor (the "Sub-processor"), the Customer agrees that Cloud-IAM may sub-process the Processing of the Customer's Personal Data.

Notwithstanding the general consent given by the Customer, Cloud-IAM shall inform the Customer of any intended changes concerning the addition or replacement of any Sub-processor within a reasonable time prior to implementation of such change. The list of the sub-Processors under the authority of Cloud-IAM is available to the Customer at https://www.cloud-iam.com/en/gdpr-sub-processor.

Where Cloud-IAM engages a Sub-processor who shall process the Customer's Personal Data, the same data protection obligations as set out in the DPA shall be imposed on the Sub-processor by Cloud-IAM.

This agreement must in particular provide for an obligation of the Sub-processor to provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of Data Protection Regulations and of the DPA.

ARTICLE 6. TRANSFER OF CUSTOMER'S PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

Cloud-IAM warranties the Customer that the Customer's Personal Data are located in France or in the European Union. Cloud-IAM undertakes not to carry out any transfer of Customer's Personal Data outside the EEA without the written consent of the Customer.

At the request of the Customer and upon instructions, Cloud-IAM shall store or transfer Personal Data to other Cloud-IAM entities and/or to Sub-processors located in countries outside the EEA ("Third Countries"). In that case and when Third Countries have not been subject to an adequacy decision of

the European Commission, Cloud-IAM undertakes that the transfer will be carried out in accordance with the Data Protection Regulations and will be subject to appropriate safeguards to guarantee a level of protection equivalent to the one guaranteed by the Data Protection Regulations, such as the signing of the Standard Contractual Clauses adopted by the European Commission and available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

The Customer hereby mandates Cloud-IAM to sign on its behalf the Standard Contractual Clauses with Cloud-IAM entities and sub-Processors located in Third Countries.

At the request of the Customer, Cloud-IAM agrees to assist the Customer to perform a transfer impact assessments to identify any gaps between the Data Protection Regulations and the laws of the Third Country and to implement the necessary supplementary measures to guarantee a level protection equivalent to the one guaranteed by the Data Protection Regulations.

ARTICLE 7. SECURITY MEASURES AND CONFIDENTIALITY OF THE PROCESSING.

Cloud-IAM shall take, insofar as this is relevant to the provision of the Services or compliance with its other obligations in the DPA, adequate measures to ensure a level of security of the Customer's Personal Data appropriate to the risk and to take into account the principles of data protection by design and by default in the execution of the DPA.

Cloud-IAM undertakes to:

a) implement all appropriate technical and organisational measures in order to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Personal Data transmitted, stored or otherwise processed and, in particular, all the measures mentioned in Appendix B;
b) respect all the instructions communicated by the Customer in relation to security and confidentiality measures that can be reasonably implemented;
c) make Customer's Personal Data accessible and consultable only to duly authorised persons;
d) ensure confidentiality of the Customer's Personal Data processed under the DPA and that all the persons authorised to process the Customer's Personal Data under the authority of Cloud-IAM (including employees and sub-Processors) undertake to respect the confidentiality of the said data or are under an appropriate statutory obligation of confidentiality.

ARTICLE 8. PERSONAL DATA BREACH NOTIFICATION.

Cloud-IAM shall notify the Customer of any Personal Data Breach without undue delay and in writing after it becomes aware of a Personal Data Breach. When the information is available to Cloud-IAM, such notification shall:

a) describe the nature of the Personal Data Breach including where possible, the categories and approximate number of the concerned Data Subjects and the categories and approximate number of Personal Data concerned;
b) communicate the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
c) describe the likely consequences of the Personal Data Breach;
d) describe the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

At the request of the Customer, Cloud-IAM also undertakes to provide the Customer with reasonable assistance and co-operation to notify the Personal Data Breach to the competent Data Protection Authority and to communicate such Personal Data Breach to the Data Subjects, in compliance with applicable Data Protection Regulations.

ARTICLE 9. RIGHTS OF THE DATA SUBJECTS.

Based on the nature of the Personal Data Processing activities, Cloud-IAM undertakes to:

a) promptly notify the Customer of any request or complaint received relating to data protection of Customer's Personal Data;
b) at the request of the Customer, provide the Customer with reasonable assistance and co-operation, to allow the Customer to respond (i) to requests presented by Data Subjects for exercising their rights (right of access, rights to rectification, erasure, limitation, portability and object), or (ii) to respond to the competent data protection authorities' requests or the Customer's Data Protection Officer requests; in particular, implement appropriate technical and organisational measures to allow the Customer to promptly satisfy in writing to any request for information of the Customer;
c) duly provide the Data Subjects with the adequate information on the Personal Data Processing operations carried out concerning their Personal Data under the Terms of Services, where requested by and at the expense of the Customer.

ARTICLE 10. DATA PROTECTION IMPACT ASSESSMENT

At the request of the Customer, Cloud-IAM undertakes to provide the Customer with reasonable assistance and co-operation to carry out an assessment of the impact of the Personal Data Processing operations carried out under the present DPA on the protection of Personal Data and to consult the competent data protection authorities, where necessary and at the expense of the Customer (based on a time and materials fee).

ARTICLE 11. RETENTION, RETURN OR DESTRUCTION OF THE PERSONAL DATA.

The Customer remains solely responsible for implementing and managing Personal Data retention periods, and undertakes to use the Product accordingly.

Without prejudice to the applicable laws and regulations Cloud-IAM undertakes to, at the end of the Terms of Services:

i. return or destroy, at the Customer's request, all Customer's Personal Data in an automated or manual way, following processes and prescriptions previously agreed between the Parties;
ii. delete all existing copies of the Personal Data unless and to the extent that Cloud-IAM is required to retain copies of the Personal Data in accordance with applicable laws;
iii. Certify the destruction of the Personal data in writing.

ARTICLE 12. DOCUMENTATION AND AUDIT

Upon prior written notice of thirty (30) business days sent by the Customer, Cloud-IAM shall disclose to the Customer the information strictly necessary to demonstrate compliance with the obligations laid down in this Terms of Services.

At the request of the Customer and once a year, Cloud-IAM undertakes to allow for and contribute to reasonable audits, including inspections, conducted by or on behalf of the Customer, for the purposes of assessing the Cloud-IAM's compliance with the Data Protection Regulations and the provisions of the DPA.

Cloud-IAM also undertakes to allow for and contribute to audits conducted by competent Data Protection Authorities.

The Customer shall have no right to view or access any systems, data, records or other information relating or pertaining to Cloud-IAM's other customers.

Any such audit by or on behalf of the Customer shall be conducted at its own costs. The Customer shall provide Cloud-IAM with a copy of the audit report.

In the event that the Customer is subject to an investigation or a request for information by a competent data protection authority and concerning any of the processing operations carried out by Cloud-IAM on behalf of the Customer, the Customer undertakes to inform Cloud-IAM as soon as possible and to satisfy such investigation or request, to the best of its ability, at the expense of the Customer, and in accordance with the procedures adopted by the data protection authority.

The Customer undertakes to comply with any confidentiality provisions, policies and/or site rules Cloud-IAM may notify to the Customer in relation to the audit.

APPENDIX 1 - PERSONAL DATA PROCESSING ACTIVITIES CARRIED OUT BY CLOUD-IAM ON BEHALF OF THE CUSTOMER

Nature of the Processing operations	[to be completed by the Customer]
Purpose(s) of Processing	[to be completed by the Customer]
Name and contact details of the Customer's Data Protection Officer (if applicable)	
Category/ies of Personal Data *At the Customer request, processing of Special Categories of Personal Data may be performed by Cloud-IAM. In such case, the Processing shall be covered by a specific addendum to the DPA to be entered into between the Customer and Cloud-IAM.*	[to be completed by the Customer]
Category/ies of Data Subjects	[to be completed by the Customer]
Location(s) of Processing operations *If the Customer requests the Personal Data to be located outside the EEA, such Processing shall be covered by a separate agreement between the Customer and Cloud-IAM.*	France or EEA Please see : https://www.cloud-iam.com/en/gdpr-sub-processor
Identity of the sub-Processor(s)	Please see: https://www.cloud-iam.com/en/gdpr-sub-processor
Duration of Processing operations	For the duration of the Terms of Services.

APPENDIX 2 – APPROPRIATE TECHNICAL AND ORGANISATIONAL MEASURES IMPLEMENTED

The following technical and organisational measures are implemented by Cloud-IAM in order to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or, or access to Personal Data transmitted, stored or otherwise processed:

People, awareness and HR:

- All recruitments follow a screening process according to the principles of the Cloud-IAM background check policy;
- In each contract each employee has Non-Disclosure Agreements clauses;
- Code of Ethics awareness training (including a test) is a yearly obligation for all employees and is to be performed through a dedicated e-learning module;
- Group IT Acceptable Use policy or local version, are shared with all employees;
- Security policy statement signed by the Management is shared with all employees;
- Cloud-IAM staff is obliged on a yearly basis to follow the Cloud-IAM Data Protection policy, Information Security and Safety training (including a test);
- Regular awareness trainings on GDPR for all employees (in addition to Cloud-IAM Data Protection policy, Information Security and Safety training);
- Access to systems is provided on a 'need to have basis' taken into account segregation of duties;
- Regular internal security audits are conducted to verify the security practices.

Physical Security and paper records:

Compliance with the Cloud-IAM Physical and Environmental Security policy:

- Access control and visitor management systems implemented for all visitors/guests;
- Physical access reviews as per defined periodicity;
- Clean desk, clear screen and follow me printing, process implemented;
- Information, which includes paper documents, handled by the data importer is classified, labelled, protected and handled according to the Cloud-IAM information classification policy;
- Except with prior specific authorization, laptops and desktops are not taken off the site;
- CCTV surveillance to protect restricted areas;
- Fire alarm and fire-fighting systems implemented for employee safety;
- Fire evacuations drills are conducted at specified frequencies;

Remote end user device are protected:

The remote users are working with laptop and desktop on Cloud-IAM secured network. Following security measures are incorporated in addition:

- Encryption of the hard disk on company assigned laptops;
- 2 Factors Authentication (PKI / Alternative);
- Centrally managed and anti-virus protection;
- Management and monitoring of the software to control an authorized software installation;
- Vendor supplied updates are installed;
- All the laptops and desktops working on the Cloud-IAM projects follow a strong overwriting process before it is reassigned;
- Login ID and password controls are implemented to access information;
- Periodic access review is implemented;
- E-mails are automatically scanned by anti-virus and anti-spam software.

Remote Access Security

2-factor authentication is used in general for remote access to the critical Cloud-IAM target systems. If the source of the remote connection is a Cloud-IAM controlled system then device authentication based on a certificate on the device is implemented. If the source is not under Cloud-IAM control, it should connect to a virtual desktop system.

Any other set up of connections needs to be upfront approved by the security department.

Generic security measures are a.o.:

- Data is only stored in the EU Data Centers or in case of laptops encrypted on the local device;
- Termination of access connection in Demilitarized Zone;
- All connectivity up to the secured area (PCI zone) is encrypted;
- Access to PCI zone only possible via strong authentication via Cloud-IAM provided security client;
- Multiple layers of firewalls & intrusion detection need to be passed;
- Access managed according to Role Based Access Control principles.

Access control to Personal Data

Employees with access to private data can only access the data that are necessary for the purpose of the activities under their responsibility. Access authorisation is provided based on the 'need to know' and 'need to access' and is either role based or name based. Access logs are in place and the responsibility for access control is assigned.

Following measures are in place:

- Obligation for employees to comply with the applicable Cloud-IAM security policies and data protection policies;
- Work instructions on handling private data;
- User (password) codes for access to Private Data;
- Differentiated access regulations (e. g. partial blocking);
- Access Logging and control;
- Controlled destruction of data media;
- Procedures for Checking compliance with procedures and work instructions are in place;
- Formalised Control frameworks and TPA to take care that not a single person can access, modify or use critical information assets without authorization or detection;

Security and confidentiality of personal data

Based on a risk assessment (and if required an additional DPIA) Cloud-IAM will ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the anonymization, pseudonymisation (e.g. tokenization) and encryption of Personal Data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- ensure a logical separation between its own data, the data of its customers and suppliers
- set up a process to keep processed data accurate, reliable and up-to-date.
- Process registers according GDPR requirements
- Access log systems' use with relevant for the purposes of being able to detect unauthorized access attempts

- Customer Data (including back-ups and archives) will only be stored for as long as it serves the purposes for which the data was collected unless there is a legal or contractual obligation to retain the data for a longer period of time.

Organization control

The Data Processor shall maintain its internal organization in a manner that meets the requirements of the applicable legislation and the Data controller requirements on data security. This shall be accomplished by:

- Internal data processing policies and procedures, guidelines, work instructions, process descriptions and regulations for programming, testing and release, insofar as they relate to the Personal Data transferred by the Controller;
- Implementing a Data Protection control framework that is audited on compliance on a yearly basis
- Having an emergency plan with procedures and allocation of responsibilities in place (backup contingency plan).