ANNEXE 1 :
DATA PROCESSING AGREEMENT

Regarding the data processing performed in the context of the Agreement (hereafter "Data processing"), Leyton acts as a Data processor ("Processor") and the Client acts as Data controller ("Controller"). The Parties agree to define the concept of an instruction as being acquired when the Processor acts in the context of the performance of this Agreement. All the terms that are defined in the General Data Protection Regulation (2016/679/EU, hereinafter to be referred to as: the "GDPR"), shall have the meaning as defined in the GDPR.

ARTICLE 1 - COMMITMENTS OF THE DATA CONTROLLER

It shall be the responsibility of the Controller to ensure that the measures for security and confidentiality offered by the Processor are in accordance with the level of care that the Controller must take with regard to its obligation for the security of the personal data for which it is responsible and that the guarantees presented by the Processor to this effect are sufficient. The legal basis of the Data processing is the legitimate interest of the Controller. The personal data that will be processed in the context of the Agreement will be collected by the Controller and communicated to the Processor based on the document requests issued by the Processor. With regard to the Data processing, the Controller guarantees that it shall comply with its obligations in terms of information of the data subjects.

ARTICLE 2 - OBLIGATIONS OF THE PROCESSOR

The Processor undertakes to take all of the appropriate measures necessary for it and for its personnel to comply with these obligations and in particular:

- not to process or consult outside of the context of the documented instructions received from the Controller, including those which concern the transfer of personal data to a country outside of the European Union - except to countries belonging to the LEYTON group - or an international organisation, unless the Processor is required to do so on the basis of an imperative provision resulting from European Union law or the law of the Member State to which it is subject. In this case, the Processor informs the Controller of this legal obligation before the processing of the data, unless the law in question prohibits such information for important reasons of public interest;

- to ensure that the persons authorized to process the personal data undertake to observe the confidentiality or are subject to an appropriate legal obligation of confidentiality;

- assists the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR.

The Processor shall keep up to date a registry of the processing activities carried out on behalf of the Controller. If a data subject contact directly the Processor to exercise of his right(s), the Processor shall inform as soon as possible the Controller and provide appropriate technical and organisational measures to assist the Controller to perform its obligation to accede to these requests.[1]

ARTICLE 3 - SECURITY

With regard to the type of data and the risks presented by the processing, and considering the state of knowledge, the cost for implementing and the character, scope, context and purposes for the processing as well as the risks for the rights and liberties of physical persons, the Processor undertakes to take all measures necessary in order to preserve the security of the data and the files, and in particular to prevent any distortion, alteration, damage, destruction, either accidentally or illicitly, any loss, disclosure and/or any access by a third party which is not authorised in advance. Consequently, the Processor shall implement appropriate technical and organisational measures in order to preserve a level adapted to the security of the data, in particular, to prevent them from being distorted or damaged, and to prevent any access that may not have been authorised in advance by the Controller. Upon request, the Processor will communicate its Security Policy to the Controller.

ARTICLE 4 - DATA BREACHES

The Processor undertakes to notify the Controller as soon as possible, and no later than 48 hours, after becoming aware of any personal data breach, or any security breach causing, either accidentally or illicitly, the destruction, loss, alteration, or unauthorised disclosure of personal data transmitted, retained or processed in any other manner, or the unauthorised access to such data when they may cause harm to the rights of the data subjects.

This notification must be sent to the Controller by electronic mail. It must, to the extent possible, specify the character and the consequences of the personal data breach as well as the measures already taken or those that are proposed in order to remedy the situation. The Processor undertakes to collaborate with the Controller in order to be able to meet its obligations in terms of notification of the supervisory authorities as well as, if necessary, the data subject.

ARTICLE 5 - SUB PROCESSORS

The list of the sub-processors, in the sense of the regulations on the General Data Protection Regulation is the following:

[1] DPO : Xavier de Marcillac, dpo@leyton.com

- Any company belonging to the LEYTON Group, some of which are located in countries outside the European Union.

The Processor may revoke, replace or appoint subsequent Sub-processors subject to the following provisions:

- impose on the sub-processor the same obligations in terms of the protection of data as those set in this annex and in the Agreement;
- inform the Controller by electronic mail in advance (except in the case of an urgent replacement) of any modifications that may affect the list of sub-processors. The Controller is required to inform the Processor of any valid reason for opposition in writing within fifteen (15) days following receipt of the electronic mail. If the Controller does not manifest its opposition by registered letter with proof of delivery within fifteen (15) days following receipt of the electronic mail from the Processor, the new sub-processor(s) shall be considered to have been accepted by the Controller. In the case of a valid opposition by the Controller, the Processor may, at its request, (i) waive the idea of using a sub-processor or (ii) take the corrective measures sought by the Controller or (iii) confirm to the Controller that it will use the sub-processor despite the Controller's opposition. In this last case, the Controller has the right to terminate the Agreement at its convenience within a period of one month following the date of receiving confirmation of the use of the sub-processor.

When its Sub-processor do not meet their obligations in terms of data protection, the Processor shall remain fully responsible towards the Controller for the performance of their obligations by the Sub-processors.

ARTICLE 6 - TRANS-BORDER FLOWS

In the event of the transfer of personal data to a third party country which does not belong to the European Union and which is not part of the LEYTON group, the Processor must obtain the prior written consent of the Controller.

With the exception of transfers within the Leyton Group[2] as well as to countries recognized by the European Commission as providing an adequate level of protection, the Processor shall provide one of the appropriate safeguards mentioned in Article 46 of the GDPR.

ARTICLE 7 - AUDIT

The Processor undertakes to collaborate in a reasonable manner and to provide to the Controller all of the information necessary in order to:

[2] Transfers within the LEYTON Group are governed by BCR, available at: https://www.leyton.com/BCR-P_FR

- demonstrate observance of their contractual obligations in terms of the processing of personal data as well as with regard to the applicable data protection regulation;
- allow the performance of an audit concerning the protection of data to be carried out by the Controller or by an authorised supervisory authority.

The audit shall not last more than two (2) working days every twelve (12) months. The Processor shall be notified by email at least 30 days in advance. The Controller shall ensure the signature of a confidentiality commitment by its auditors, who may not be a direct competitor of the Processor or one of its former employees. The audit must not interfere with the capacity of the Processor to provide its services in accordance with the Agreement. If the conclusions of certain audits contain recommendations which seek the modification or the improvement of the audited procedures and services, the implementation of these recommendations between the parties shall be discussed jointly by the parties and shall, if necessary, be subject to an amendment to the Agreement.