DATA PROCESSING AGREEMENT (DPA)

This Data Processing Agreement ("**DPA**") forms part of CLIENT general terms and conditions of purchase accepted by PROVIDER (the "**Terms and Conditions**"), and shall apply to all services carried out by PROVIDER on behalf of CLIENT under the purchase order or any other relevant documentation (the "**Order**") executed pursuant to the agreement between the Parties (the "**Services**").

This DPA details the Parties' respective obligations regarding the protection of Personal Data, associated with the Processing of Personal Data on behalf of CLIENT, by PROVIDER. The measures provided for in this DPA shall apply to any and all activities associated with the Services. The provisions set forth below apply where PROVIDER processes Personal Data for the purposes of performing the Services.

Where the Services provided under the Order benefit affiliates of CLIENT either directly or through the signature of any relevant documentation (e.g. implementation agreement, statement of work, service order, etc.), the Parties expressly agree that each CLIENT affiliate shall be regarded as a Controller independently in its own right.

ARTICLE 1. DEFINITIONS

Under this DPA, the Parties agree that the terms "**Personal Data Breach**", "**Data Subject**", "**Personal Data**", "**Controller**", "**Processor**", "**Processing**", "**Supervisory Authority**" and "**Third Party(ies)**" shall have the meaning assigned to them in Regulation 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 (the "**GDPR**").

In addition:

"Applicable Data Protection Law" means the personal data protection laws, rules and regulations applicable in the country where Controller is established. In particular, the GDPR shall apply to all Processings falling within its scope, and all additional regulations and rules in force in the relevant Member State(s) of the European Union applicable to the Processing(s).

"GDPR" means Regulation 2016/679/EU of the European Parliament and Council of 27 April 2016 relating to the protection of natural persons regarding the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC.

"Subprocessor" means any natural or legal person engaged by Processor only for the performance of the Processing under the Order and as authorised in advance, either generally or specifically, as agreed between the Parties, in writing (including by email) by Controller.

"Third Party Country" means any country, territory or specified sector within that country outside of the European Economic Area (EEA) that is not recognized by the European Commission or any competent authority (including a Supervisory Authority) as ensuring an adequate level of protection.

ARTICLE 2. PARTIES' RESPECTIVE ROLES AND RESPONSIBILITIES

The Parties agree that, for the purposes of the Order, CLIENT is the Controller and PROVIDER processes Personal Data as a Processor. Accordingly, Processor shall process the Personal Data exclusively for the purpose of providing the Services under the Order, with Controller.

Processor shall comply with Applicable Data Protection Law when performing its obligations under this DPA, in such a way as to not expose Controller to any violation of Applicable Data Protection Law.

2.2.1. Compliance with Controller's instructions

Processor shall process Personal Data on behalf of Controller exclusively in order to provide the Services for the purposes defined by Controller as well as in accordance with the documented instructions received from Controller (as set out the Order), unless Processor is required to do so by Union or Member State law to which Processor is subject. Notably, Processor shall not modify, amend or alter the contents of the Personal Data unless expressly instructed to do so in writing (including by email) by Controller.

Controller shall be entitled to supplement its instructions in writing (including by email) to Processor from time to time during the course of the performance of the Services.

If Processor cannot comply, for whatever reason, with any of the provisions set out in this Article 2.2, Processor must inform Controller promptly of its inability to comply, and Controller will be entitled to immediately and automatically suspend any Processing and/or terminate the Order, without incurring any penalties or charges.

2.2.2. Compliance in case of subcontracting/ subprocessing

Processor shall only disclose or permit the disclosure of Personal Data to any Third Party, and/or subcontract all or part of the Processing to any Subprocessor, if it has obtained the prior specific written approval of Controller (including by email) and shall only do so on the basis of a written agreement with obligations no less onerous than Processor's obligations under the DPA and after having ensured that the Subprocessor in question provides sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of Applicable Data Protection Laws, of the Agreement (including this DPA) and of the Order. Such subcontracting shall not release Processor from its responsibility for its obligations under the General Terms and conditions (including this DPA) and the Order. Processor remains solely responsible for the work and activities of such Subprocessor and liable for its acts and omissions.

2.2.3. Obligation to assist Controller

The Parties agree that, Processor, as a professional, is required to assist Controller in the implementation of the Processing and of all operations allowing to ensure compliance of the processing with Applicable Data Protection Law. In this respect, and in accordance with Applicable Data Protection Law, Processor shall, upon request from Controller, provide assistance in the management of Data Subject requests, of relationships with Supervisory Authorities and in the completion of Data Protection Impact Assessments (DPIA) or any obligation resulting from Applicable Data Protection Law. Processor shall make its registers of Processing activities available to any competent Supervisory Authority and/or to the Controller.

2.2.4. Management of persons granted access to Personal Data – confidentiality and training

Processor shall ensure that the authorised persons who are granted access to the Personal Data within the framework of the Services are properly trained on the Processing of Personal Data and are only granted access to such Personal Data on a need-to-know basis subject to obligation of confidentiality or secrecy who have been duly instructed and trained about Applicable Data Protection Law. Processor shall also take steps to ensure that the authorised persons only process Personal Data in accordance with the terms of this DPA, unless required to do so by Union or Member State law, in which case, Processor shall immediately inform Controller, unless prohibited by applicable law.

2.2.5. Liability

Processor shall be fully accountable and liable in the event of any breach of its obligations under this DPA and/or non-compliance with the Applicable Data Protection Law. Processor shall indemnify and hold Controller harmless for any breach of its obligations under this DPA, without being subject to the limitation of liability set forth in the Terms and Conditions.

ARTICLE 3. SECURITY AND CONFIDENTIALITY MEASURES

Processor guarantees that it will take, implement and maintain during the entire term of the Services all appropriate technical and organizational security measures which shall ensure the confidentiality, integrity, availability and resilience of the processing systems and services, and regularly update them and protect Personal Data particularly against any accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access. It shall also implement technical and organizational measures, to ensure that it has, at all times, the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident and that it will regularly test the effectiveness of the technical and organizational security measures implemented as per the above by means of an audit. Processor shall communicate on a regular basis and at least once a year a summary report of the effectiveness of these measures. The provision of such reports shall not preclude Controller from its right to conduct Audits as provided for in section 7 below.

ARTICLE 4. TRANSFERS OF PERSONAL DATA

For the purposes of this section, the Member States of the EEA and all countries which have been recognized as providing an adequate level of protection to Personal Data by the European Commission by means of an adequacy decision shall be regarded as a single jurisdiction (hereinafter “EEA Jurisdiction”).
In cases where Processor intends to implement a transfer of Personal Data outside of EEA Jurisdiction (including to a Subprocessor) to a Third Party Country after having obtained written approval from Controller, it shall ensure that adequate safeguards are, if necessary, implemented and maintained for the entire term of the Order, in accordance with Applicable Data Protection Law prior to implementing such transfer, including, notably, applicable standard contractual clauses for the transfer of Personal Data between Controllers and Processors as set out in the European Commission decision of February 5, 2010 (C (2010) 593) or in any decision amending or replacing such decision. Controller hereby expressly mandates Processor to enter into any relevant agreements to ensure such adequate level of protection is afforded. For this purpose, the Processor also warrants that its Subprocessors are bound by similar obligations to implement adequate safeguards in case of transfer of Personal Data outside EEA Jurisdiction.

ARTICLE 5. PERSONAL DATA BREACH

In the event of a Personal Data Breach arising during the performance of the Services by Processor, Processor shall, at its own costs notify Controller about the Personal Data Breach without undue delay after becoming aware of it and in any case within twenty-four (24) hours of becoming aware of it. The notification by Processor shall include at least information about the nature of the Personal Data Breach (including categories and approximate number of Data Subjects concerned, and categories and approximate number of Personal Data records concerned), the name and contact details of Processor’s data protection officer or other contact point, the likely consequences of the Personal Data Breach and the measures taken or proposed to be taken to address the Personal Data Breach including, where appropriate, measures to mitigate its possible adverse effects.

In the event that such information only becomes available to Processor progressively, it shall communicate such information to Controller immediately after it has obtained it. Processor shall provide all relevant information as reasonably requested by CLIENT without undue delay and Processor shall implement, at its own costs and in concertation with CLIENT all necessary actions to mitigate, limit, compensate and prevent the Personal Breach from occurring again in the future.

Unless provided otherwise, Controller is responsible for informing Data Subjects affected by a Personal Data Breach. Processor shall not notify Personal Data Breaches to Data Subjects unless it has been expressly and specifically instructed by Controller. In any case, Processor shall assist Controller in accordance with the provisions of article 2.2.3 above.

ARTICLE 6. OBLIGATION TO INFORM CONTROLLER

Processor shall promptly notify Controller and shall answer appropriately and without delay any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless otherwise legally prohibited and in compliance with Applicable Data Protection Laws as well as any notification received from a Supervisory Authority alleging infringement of the Applicable Data Protection Law, or of the exercise by a Supervisory Authority of any of its powers in relation to the provision of the Services.

Finally, Processor shall provide prior notification to CLIENT regarding any significant changes brought to the Services having an impact on the Processing in order to allow CLIENT to assess the impact of the changes.

ARTICLE 7. AUDIT

Controller shall be entitled to carry out any controls or audits it deems relevant regarding Processor's compliance with its obligations under this DPA. Such audits and controls may be carried out also at the premises and/or on the systems of possible Subprocessors to which Processor has subcontracted all or part of the Processing according to the provisions of article 2.2.2 above and shall take place in accordance with the audit provisions set out in the Terms and Conditions.

ARTICLE 8. TERMINATION OF THE ORDER / RESTITUTION AND OR DESTRUCTION OF THE PERSONAL DATA

The duration of the Processing shall not exceed the term of the Order. Upon termination of the Order, for whatever reason, Processor shall cease processing any Personal Data on behalf of Controller. In this respect, Processor shall, in accordance with the instructions received from Controller, either delete or return the Personal data it has received.