TERMS OF PURCHASE – DATA PROCESSING AGREEMENT

Incorporation into Terms and Conditions. This Data Processing Agreement ("DPA") forms part of CLIENT's general terms and conditions of purchase accepted by PROVIDER (the "Terms of Purchase" or "ToP").

Scope of Application. This DPA shall apply to all services and associated activities 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**"), to the extent PROVIDER processes Personal Data for the purposes of performing the Services for CLIENT (the "**Processing Activities**").

Definitions. Where this DPA uses the terms defined in Regulation (EU) 2016/679 (the "GDPR"), those terms shall have the same meaning as in the GDPR. In this DPA, "**Applicable DP Laws**" shall mean (i) the GDPR and (ii) the applicable local law(s) and regulations on protection of Personal Data applicable to the Processing Activities, as amended from time to time.

Purpose of the DPA. This DPA sets forth the Parties' respective obligations regarding the protection of Personal Data, associated with the Processing Activities.

Status of CLIENT Affiliates. Where the Services benefit CLIENT Affiliates (either directly or through the execution of separate contractual documentation such as implementation agreement, statement of work, service order, etc.), each CLIENT Affiliate shall be regarded as an independent Data Controller. The Parties and/or CLIENT Affiliate benefiting from the Service may supplement this DPA with additional terms as required by Applicable Data Privacy Laws.

1. GENERAL OBLIGATIONS.

1.1. Compliance. Each Party shall comply with its respective obligations as Data Processor and Data Controller under Applicable DP Laws. If PROCESSOR cannot comply with this DPA and/or Applicable DP Laws, it shall notify CONTROLLER without unreasonable delay once aware of such inability, in which case, CONTROLLER shall be entitled to suspend the Processing Activities and/or terminate the Order, without incurring any penalties or charges.

1.2. CLIENT Instructions. PROCESSOR shall process Personal Data (i) only for the purpose(s) defined by CLIENT as part of the provision of the Services and/or (ii) only on documented instructions from CONTROLLER by way of the Order - including subsequent reasonable instructions throughout the performance of the Agreement. PROCESSOR shall inform promptly CONTROLLER if, in the PROCESSOR's opinion, such instructions infringe Applicable DP Laws.

1.3. Changes to the instructions. CONTROLLER may adapt its instructions at no further costs and without unreasonable delay (i) to remediate any discovered breach of Applicable DP Laws or of this DPA and/or (ii) implement changes of Applicable DP Laws, or (iii) in case of suspected or confirmed Personal Data Breach. Any other change of instructions shall be subject to applicable change control provisions under the Agreement. PROCESSOR shall implement such changes without further costs unless agreed between the Parties in accordance with the Agreement and without unreasonable delay.

1.4. Legal requirements. PROCESSOR may process Personal Data for other purposes than the ones provided in this DPA and the Agreement to the extent this is necessary for PROCESSOR to comply with its legal obligations, such as a request for access by governmental authorities. PROCESSOR shall inform CONTROLLER in writing before such processing - unless prohibited by applicable laws.

1.5. Audit & Accountability. PROCESSOR shall make available to the CONTROLLER all information necessary to demonstrate compliance with this DPA and Applicable DP Laws. PROCESSOR shall allow, collaborate with and contribute to audits of the Processing Activities subject to the conditions set forth in the Agreement. Such audit(s) shall be conducted by CONTROLLER or by an independent auditor of CONTROLLER's choice, shall be documented and may include on-premises inspections. In case of breach identified by the auditor, PROCESSOR shall implement relevant actions to remediate the breach without undue delay. Where applicable, PROCESSOR shall make its registers of processing activities available to any competent Supervisory Authority and/or to the CONTROLLER.

1.6. Records of Processing Activities. PROCESSOR shall maintain, update and keep available to CONTROLLER, a record of the Processing Activities in accordance with article 30 (2) of the GDPR

1.7. Accountability. Each Party shall be able to demonstrate its compliance with its own obligations under the DPA and Applicable DP Laws. The PROCESSOR shall address promptly and adequately any inquiries from the CONTROLLER about the Processing Activities.

2. SECURITY AND CONFIDENTIALITY

2.1. Security. PROCESSOR shall implement maintain and keep updated all appropriate technical and organizational measures to ensure continuously the security, confidentiality, integrity, availability of the Personal Data and to protect them against any accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access. Such measures shall include the ability to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident. PROCESSOR may implement changes to these measures without CONTROLLER's prior approval exclusively to maintain or increase the level of security.

2.2. Regular testing. PROCESSOR shall regularly test the effectiveness of these measures by means of regular audits consistent with internationally recognized standards (e.g. ISAE 3402, ISO 270001, etc.). A report or summary of such audits shall be kept available at all times to CONTROLLER and communicated once a year, without prejudice to CONTROLLER's right to conduct audit as set forth in section 1.5.

2.2. Confidentiality. PROCESSOR shall grant access to the CONTROLLER's Personal Data to its personnel only to the extent that (i) it is strictly necessary for the performance of the Services, (ii) such personnel is under a legal, statutory or contractual obligation of confidentiality, (iii) such personnel has been duly trained regarding the protection of Personal Data.

3. SUB-PROCESSING

"SUBPROCESSOR(S)" definition. For the purposes of this DPA, "**SUB-PROCESSOR(S)**" shall mean any person, whether a third-party subcontractor or a PROCESSOR Affiliated Company engaged by PROCESSOR, for the performance of the Processing Activities.

General Authorization. PROCESSOR is hereby authorized to engage the SUB-PROCESSORS listed in the most up-to-date applicable public documentation that PROCESSOR keeps available at all times to its Clients, such as its corporate website. PROCESSOR shall communicate such list or a link to such list to CONTROLLER prior to the execution of the Order. Any substantial change to this list shall be subject to prior written notice to the CONTROLLER at least thirty (30) calendar days before the change. CONTROLLER may object to such changes on reasonable grounds.

Obligations of SUB-PROCESSOR(S). SUB-PROCESSORS shall be contractually bound to PROCESSOR by substantially equivalent obligations as those set forth by this DPA. PROCESSOR shall ensure that SUB-PROCESSORS implement appropriate measures to meet the requirements of Applicable DP Laws and this DPA, including by way of regular audits. At CONTROLLER's written request, PROCESSOR shall provide – in a redacted form if needed - a copy of sub-processing agreements and audit reports.

Liability of SUB-PROCESSOR(S). PROCESSOR shall remain fully liable to CONTROLLER for the performance of SUB-PROCESSORS' obligations. PROCESSOR shall promptly notify CONTROLLER in writing should SUB-PROCESSOR(s) fail to comply with their data protection obligations.

Third-party beneficiary clause with SUB-PROCESSOR(S). PROCESSOR shall include in its contract with the SUB-PROCESSOR(S) a third-party beneficiary clause whereby - in the event PROCESSOR has factually disappeared, ceased to exist in law or has become insolvent, CONTROLLER has the right to instruct the SUB-PROCESSOR to erase or return the Personal Data.

4. DATA TRANSFERS

"THIRD COUNTRY" definition. For the purposes of this DPA, THIRD COUNTRY shall mean any country outside the European Economic Area ("EEA") identified by Applicable DP Law as not ensuring an adequate level of protection of Personal Data according to its legislation, but in which Personal Data can be transferred subject to specific safeguards.

“SCCs” definition. The SCCs shall mean the Commission implementing decision (EU) 2021/914 of 4 June 2021, on standard contractual clauses for the transfer of Personal Data to THIRD COUNTRIES pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

“DPF” definition. The U.S./E.U. Data Privacy Framework recognized as offering an adequate level of protection under Decision of 10/07/23 of the European Commission.

4.1. Transfers from CONTROLLER to PROCESSOR. If the Processing Activities involve Personal Data transfer(s) from CONTROLLER located in the E.U./E.E.A to PROCESSOR located in a THIRD COUNTRY, Module 2 (“Controller-to-Processor”) of the SCCs (i) is included herein by reference, (ii) form part of this DPA and (iii) is applicable to such transfers. The Parties agree to (i) select the Option 2 “General Written Authorization” with a thirty (30) calendar days period in Clause 9 (Use of sub-processors), (ii) withdraw Clause 11 (Redress), (iii) apply the laws of France in Clause 17.

4.2. Transfers from PROCESSOR TO CONTROLLER. To the extent that the Processing Activities involve transfers of Personal Data from the PROCESSOR or SUB-PROCESSOR located in the EEA to a CONTROLLER entity located in a THIRD COUNTRY, the Parties agree that Module 4 (“Processor-to-Controller”) of the SCCs (i) are included herein by reference, (ii) form part of this DPA and (iii) are applicable to such transfers. With regards to SCCs options, the Parties agree to (i) withdraw Clause 11 (Redress), (ii) apply the laws of France in Clause 17 (Governing Law).

4.3. Data transfers to SUB-PROCESSOR & PROCESSOR Affiliates. In case of transfers of Personal Data from PROCESSOR to a SUB-PROCESSOR and/or PROCESSOR Affiliates located in a THIRD-COUNTRY, PROCESSOR warrants that adequate safeguards (such as Module 3 of the SCCs or Binding Corporate Rules or the onward transfer principles of the DPF) are implemented.

4.4. Update to the SCCs. The Parties shall notify each other without undue delay of any event that could materially affect the validity of the SCCs. In such case, the Parties shall promptly discuss the implementation of alternative safeguards. Should the Parties fail to agree on such safeguards, CONTROLLER may terminate the Agreement without prior notice. Should the SCCs be updated, and to the extent the new SCCs remain consistent with this DPA, the new SCCs shall replace the former version of the SCCs in this DPA on the day their use becomes mandatory.

5. **ASSISTANCE AND COOPERATION**

6.1. Assistance. PROCESSOR shall provide reasonable assistance to CONTROLLER’s obligations (i) to carry out a privacy impact assessment if needed, (ii) consult or obtain authorization from the competent Supervisory Authority/ies where applicable, (iii) to ensure that Personal Data is accurate and up-to-date, (iv) to manage and respond in due time to Data Subject requests, (v) to respond promptly to Supervisory Authority inquiries pertaining the Processing Activities, including PROCESSOR’s evidence of compliance with Applicable DP Laws.

6.2. Supervisory Authorities inspections. In case of inquiries or inspections by a Supervisory Authority against PROCESSOR regarding the Processing Activities, PROCESSOR shall promptly and no later than five (5) business days following notification of such inquiry, notify CONTROLLER, to the extent authorized under applicable law, and duly cooperate to said inquiries and inspections.

6.3. Legal requests. PROCESSOR shall promptly notify CONTROLLER and answer appropriately without delay to any legally binding request for Personal Data disclosure by a law enforcement authority, unless legally prohibited and in compliance with Applicable Data Protection Laws

6. **DATA BREACH**

7.1. Definition. In the event of a Personal Data Breach arising during the performance of the Services impacting CLIENT Personal Data, PROCESSOR shall provide diligent assistance to CONTROLLER to comply with its obligations under Applicable DP Laws, in particular regarding CONTROLLER’s obligation to (i) notify where applicable the competent Supervisory Authority/ies and Data Subjects (ii) obtain data about the event including the nature of the impacted Personal Data and the categories/volume of impacted Data Subjects, (iii) determine the consequences of the breach and (iv) determine the relevant remediation or minimization and prevention measures.

7.3. Notification*.* PROCESSOR shall notify CONTROLLER within 48 hours after becoming aware of a DATA BREACH, with all relevant information related to the DATA BREACH and/or as reasonably requested by CLIENT, including those required under Applicable DP Laws. Where information becomes available to PROCESSOR sively, it may be provided in phases without further undue delay. PROCESSOR shall bear all costs associated with the above if the DATA BREACH stems from an act of omission of PROCESSOR. PROCESSOR shall implement at its own costs all necessary actions to mitigate, limit and prevent the Personal Breach from occurring again.

7. SUSPENSION / TERMINATION

8.1. Suspension right. In case of breach by PROCESSOR of its obligations under this DPA or Applicable DP Law, CONTROLLER may suspend the Processing Activities by PROCESSOR until the breach is remediated, without prejudice to CONTROLLER's termination rights under the ToP.

8.2. Deletion and restitution. The Processing Activities by PROCESSOR shall cease upon termination of the Order. Upon Controller's request, PROCESSOR shall either delete or return the Personal Data, including any copies unless required by Applicable DP Law (iii) keep available evidence of such operations and continue to ensure compliance with this DPA until deletion or restitution is complete.

8. FINAL PROVISIONS

9.1. Contractual Personal Data. The Parties acknowledge that, for the purposes of managing the contractual relationship and complying with applicable regulatory requirements, they may communicate to each other Personal Data concerning their employees (such as the name, contact details etc.) herein after "**Contractual Personal Data**". For that purpose, each Party shall be deemed as independent Controller and carry out its own processing activities in accordance with its obligations under Applicable DP Laws. The Parties agree that the transfers of Contractual Personal Data from the EEA to a THIRD COUNTRY shall be governed by the most up-to-date SCCs Module 1 included herein by reference and forming part of this DPA.

9.2. Pre-collected Personal Data. Should the Services involve the Processing of Personal Data collected by PROCESSOR outside the scope of the Agreement or licensed to PROCESSOR by a third-party, PROCESSOR, as Independent Controller, warrants that such Personal Data have been obtained in accordance with Applicable DP Law and can be lawfully processed as part of the Services. PROCESSOR shall solely determine whether consent collection and/or supplemental privacy notices are required for the performance of the Services, in which case CONTROLLER shall provide reasonable cooperation. Transfers of such Personal Data from EEA to a THIRD COUNTRY shall be governed by the SCCs Module 1 included herein by reference.

9.3. Liability. Each Party shall be fully liable of its own Processing activities for which it acts as an independent Controller in accordance with its respective obligations under this DPA and/or Applicable DP Laws. Unless the Agreement provides a specific liability mechanism regarding data protection obligations, PROCESSOR shall be fully accountable and liable in the event of any breach under this DPA without being subject to any limitation or exclusions of liability. If the Parties both contributed to the failure that gave rise to the same damage, their liability shall be shared *pro rata* their contribution.

9.4. Changes to the services. PROCESSOR shall provide prior notification to CLIENT regarding any significant changes brought to the Services having an impact on the Processing to allow CLIENT to assess the impact of the changes.

9.5. Point of contact. PROCESSOR shall provide a point of contact to CONTROLLER to manage inquiries regarding Personal Data matters within 15 days as of performance of the Agreement.