

Additional Definitions:

- 1.1 **"Data Protection Laws"** means any applicable law relating to the processing, privacy and/or use of Personal Data, as applicable to either party of the Services, including:
- The GDPR;
 - The Data Protection Act 2018;
 - Any laws which implement any such laws;
 - Any laws that replace, extend, re-enact, consolidate or amend any of the foregoing; and
 - All guidance, guidelines, codes of practice and codes of conduct issued by any relevant Supervisory Authority relating to such Data Protection Laws (in each case whether or not legally binding).
- 1.2 **"Data Subject"**, **"Personal Data"** and **"Personal Data Breach"** all have the meanings given in applicable Data Protection Laws from time to time;
- 1.3 **"GDPR"** mean the General Data Protection Regulation, Regulation (EU) 2016/679;
- 1.4 **"Protected Data"** means Personal Data received from or on behalf of the Company, or otherwise obtained in connection with the performance of the Supplier's obligations under the agreement and/or Purchase Order;
- 1.5 **"Sub-Processor"** means any agent, sub-supplier or other third party engaged by the Supplier (or by any other Sub-Processor) for carrying out any processing activities in respect of the Protected Data;
- 1.6 **"Supervisory Authority"** means any regulator, authority or body responsible for administering Data Protection Laws;
- 1.7 **"Supplier Personnel"** means all employees, officers, staff, other workers, agents and consultants of the Supplier, its Affiliate and any of their sub-suppliers or sub-processors who are engaged in the performance of the Services from time to time;
1. **DATA PROTECTION**
- 1.1 The Supplier warrants that it shall, and shall ensure its Sub-Processors and Supplier Personnel shall, at all times comply with all Data Protection Laws in connection with the processing of Protected Data and the provision of the Services and shall not by any act or omission cause the Company (or any other person) to be in breach of any of the Data Protection Laws. Nothing in the agreement or the Purchase Order relieves the Supplier of any responsibilities or liabilities under Data Protection Laws.
- 1.2 The Supplier shall indemnify and keep indemnified the Company against all losses, claims, damages, liabilities, fines, interest, penalties, costs, charges, sanctions, expenses, compensation paid to Data Subjects (including compensation to protect goodwill and ex gratia payments), demands and legal and other professional costs (calculated on a full indemnity basis and in each case whether or not arising from any investigation by, or imposed by, a Supervisory Authority) arising out of or in connection with any breach by the Supplier of this Clause 1.
- 1.3 The Supplier shall only process (and shall ensure Supplier Personnel only process) the Protected Data in accordance with Clause 1, the Purchase Order, this agreement, and the Company's written instructions from time to time except where otherwise required by applicable law (and in such a case shall inform the Company of that legal requirement before processing, unless applicable law prevents it doing so on important grounds of public interest). The Supplier shall immediately inform the Company if any instruction relating to the Protected Data infringes or may infringe any Data Protection Laws.
- 1.4 The Supplier shall at all times implement and maintain appropriate technical and organisational measures to protect Protected Data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access. Such technical and organisational measures shall be at least equivalent to the Company's technical and organisational measures and shall reflect the nature of the Protected Data.
- 1.5 The Supplier shall:
- ensure that access to Protected Data is limited to the authorised persons who need access to it to supply the Services and who are subject to a binding and enforceable written contractual obligation to keep the Protected Data confidential;
 - not permit any processing of Protected Data by any agent, subcontractor or other third party (except its own employees that are subject to an enforceable obligation of confidence with regards to the Protected Data) without the prior specific written authorisation of that Sub-Processor by the Company and only then subject to such conditions as the Company may require and shall remain fully liable to the Company for all the acts and omissions of each Sub-Processor and each of the Supplier Personnel as if they were its own; and
 - prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, appoint each Sub-Processor under a binding written contract containing the same obligations as under this Clause 1.5 in respect of Protected Data that is enforceable by the Supplier and ensure each such Sub-Processor and Supplier Personnel complies with all such obligations.
- 1.6 The Supplier shall (at its own cost and expense):
- promptly provide such information and assistance (including by taking all appropriate technical and organisational measures) as the Company may require in relation to the fulfilment of the Company's obligations to respond to requests for exercising the Data Subjects' rights under the Data Protection Laws;
- provide such information, co-operation and other assistance to the Company as the Company requires (taking into account the nature of processing and the information available to the Supplier) to ensure compliance with the Company's obligations under Data Protection Laws, including with respect to:
 - security of processing;
 - data protection impact assessments (as such term is defined in Data Protection Laws);
 - prior consultation with a Supervisory Authority regarding high risk processing; and
 - any remedial action and/or notifications to be taken in response to any Personal Data Breach and/or any complaint or request relating to either party's obligations under Data Protection Laws relevant to this CONTRACT, including (subject in each case to the Company's prior written authorisation) regarding any notification of the Personal Data Breach to supervisory authorities and/or communication to any affected Data Subjects;
 - record and refer all requests and communications received from Data Subjects or any Supervisory Authority to the Company which relate (or which may relate) to any Protected Data promptly (and in any event within seventy two (72) hours of receipt) and shall not respond to any without the Company's express written approval and strictly in accordance with the Company's instructions unless and to the extent required by law.
- 1.7 The Supplier shall not process and/or transfer, or otherwise directly or indirectly disclose, any Protected Data in or to countries outside the European Economic Area without the prior written consent of the Company (which may be refused or granted subject to such conditions as the Company deems necessary).
- 1.8 The Supplier shall maintain complete, accurate and up to date written records of all categories of processing activities carried out on behalf of the Company. Such records shall include all information necessary to demonstrate its and the Company's compliance with this clause 1, the information referred to in Articles 30(1) and 30(2) of the GDPR and such other information as the Company may reasonably require from time to time. The Supplier shall make copies of such records available to the Company promptly (and in any event within seventy two (72) hours) on request from time to time.
- 1.9 The Supplier shall (and shall ensure all Sub-Processors and Supplier Personnel shall) promptly make available to the Company (at the Supplier's cost) such information as is required to demonstrate the Supplier's and the Company's compliance with their respective obligations under this clause 1 and the Data Protection Laws, and allow for, permit and contribute to audits, including inspections, by the Company (or another auditor mandated by the Company) for this purpose at the Company's request from time to time. The Supplier shall provide (or procure) access to all relevant premises, systems, personnel and records during normal business hours for the purposes of each such audit or inspection upon reasonable prior notice (not being more than forty eight (48) hours) and provide and procure all further reasonable co-operation, access and assistance in relation to any such audit or inspection.
- 1.10 The Supplier shall promptly (and in any event within twenty four (24) hours):
- notify the Company if it (or any of its Sub-Processors or Supplier Personnel) suspects or becomes aware of any suspected, actual or threatened occurrence of any Personal Data Breach in respect of any Protected Data; and
 - provide all information as the Company requires to report the circumstances referred to in clause 1.10(a) to a Supervisory Authority and to notify affected Data Subjects under Data Protection Laws.
- 1.11 The Supplier shall (and shall ensure that each of the Sub-Processors, and Supplier Personnel shall) without delay (and in any event within seventy two (72) hours), at the Company's written request, either securely delete or securely return all the Protected Data to the Company in such form as the Company requests after the earlier of:
- the end of the provision of the relevant Services related to processing of such Protected Data; or
 - once processing by the Supplier of any Protected Data is no longer required for the purpose of the Supplier's performance of its relevant obligations under this CONTRACT, and securely delete existing copies (except to the extent that storage of any such data is required by applicable law and Supplier is processing the Protected Data as a data controller in accordance with the Data Protection Laws, in which case the Supplier shall inform the Company).
- 1.12 This Clause 1 shall survive termination or expiry of this Purchase Order for any reason.