(TO BE PRINTED ON COMPANY LETTERHEAD & SIGNED)

By agreeing to the below terms and condition, You acknowledge that You have carefully read and fully understands this DPA, and each agrees to be bound by the terms of this DPA.

This Data Processing Agreement ("DPA") forms part of the Agreement/business terms and conditions/purchase order/Order Form or any other document ("Principal Agreement") in respect to the business transaction entered into between You and Infostretch Corporation (together with its Affiliates, "Apexon"), pursuant to which You shall Processes certain Personal Data (as defined below). This DPA sets out the Parties' obligations with regard to the Processing of such Personal Data and the Parties agree as follows:

1. **DEFINITIONS**

Capitalized terms not otherwise defined below shall have the meaning given to them in the Agreement.

"**Affiliates**" means with respect to Apexon, any entity that owns or controls, is owned or controlled by, or is or under the common control or ownership of Apexon, where "control" is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity.

"**Applicable Law**" means any applicable (a) law or regulation, mandatory guidance, or code of practice in force from time to time in any applicable jurisdiction; or (b) judgment or any other requirement of any relevant court or regulatory authority.

"**Data Protection Law**" means all applicable laws, guidelines relating to the use, protection and privacy of Personal Data (including, without limitation, the privacy of electronic communications) from time to time.

"**Data Subject**" means the individual whose Personal Data is Processed by You pursuant to the Agreement and this DPA.

"**Personal Data**" means any and all data (regardless of format) that (i) identifies or can be used to identify, contact or locate a natural person, or (ii) pertains in any way to or could be reasonably associated with an identified natural person. Personal Data includes obvious identifiers (such as names, addresses, email addresses, phone numbers and identification numbers) as well as biometric data, "personal data" (as defined in the Digital Personal Data Protection (DPDP) Act, 2023 and GDPR,), "personal information" (as defined in the CCPA), and any and all information about an individual's computer or mobile device or technology usage, including (for example) IP address, MAC address, unique device identifiers, unique identifies set in cookies, and any information passively captured about a person's online activities, browsing, application or hotspot usage or device location.

"**Process**," "**Processes**," "**Processing**," and "**Processed**" means any operation or set of operations which is performed on data or sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"**Security Incident**" means (a) any act or omission that materially compromises Personal Data or the safeguards put in place by You (or Your Sub-Processors) or by Apexon should You have access to Apexon's systems that relate to the protection of Personal Data; (b) a breach of Personal Data under Data Protection Law; or (c) receipt of a complaint in relation to the privacy practices of You or a breach or alleged breach of this DPA. "Materially compromises" includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

"**Sub- Processor**" means any third party (but excluding Your employee or any employee of Your sub-contractors) appointed by or on behalf of You to Process Personal Data on behalf of Apexon in connection with the Agreement and this DPA.

2. **PROCESSING**

2.1 You warrant and undertakes that You will: (a) Process the Personal Data only for an authorized business purpose on the documented instructions of the Apexon (including as set out in the Principal Agreement

and this DPA), unless otherwise required by Applicable Law, in which case You shall, to the extent permitted by Applicable Law, inform Apexon of that legal requirement before the relevant Processing of Personal Data; (b) notify Apexon if You believes any such instruction violates Data Protection Law, unless prohibited from doing so by Applicable Law; and (c) Process the Personal Data in accordance with Data Protection Law.

2.2 Apexon does not provide Personal Data in exchange for monetary or other valuable consideration. Any provision of Personal Data from Apexon to You does not constitute a "sale" under the applicable Data Protection laws. You agrees that: (a) you are "service provider" under the applicable Data Protection laws; (b) You will not retain, use, or disclose any Personal Data provided by or on behalf of Apexon for any purpose other than to: (i) provide the services under the Principal Agreement; and (ii) use the Personal Data for internal operational purposes to verify, maintain, or improve the quality or safety of the services provided that the use of such Personal Data is reasonably necessary and proportionate to perform such internal operational activity, and not for commercial purposes to benefit third parties; and (c) You are prohibited from: (i) selling the Personal Data; and (ii) retaining, using, or disclosing the Personal Data outside of the direct business relationship with Apexon.

3. SUB-PROCESSING

3.1 You may engage any Sub-Processors only after prior written consent of Apexon on its terms and conditions including entering into a written agreement with your Sub-Processors. Authorizing any Sub-Processor shall be at the sole discretion of Apexon.

3.2 You shall remain responsible to Apexon for its Your Sub-Processors (and their sub-Processors, if applicable) failure to perform their obligations with respect to the Processing of Personal Data.

4. CONFIDENTIALITY AND LIMITED PROCESSING

4.1 You shall Process Personal Data only for the purposes for which such Personal Data is made available pursuant to the terms of the Agreement, and shall not retain, use, sell, rent, transfer, distribute, disclose, make available, or otherwise Process Personal Data for Your own or any third party's purposes without Apexon's written permission except as otherwise expressly required by Applicable Law, in which case You shall, to the extent permitted by Applicable Law, inform Apexon of that legal requirement before the relevant Processing of Personal Data and provide Apexon with sufficient information for Apexon to seek a protective order or other protective measure for the Personal Data.

4.2 You shall ensure that Personal Data is disclosed only on a need-to-know basis and that any person to whom any Personal Data is disclosed (including any Sub-You) agrees to maintain the confidentiality and security of such Personal Data or is under an appropriate obligation of confidentiality.

5. INFORMATION SECURITY

5.1 You confirm and can evidence that You have implemented reasonable and appropriate technical and organizational measures that provide an adequate level of security and protects Personal Data against reasonably foreseeable internal and external risks to the security, confidentiality, availability, and integrity of Personal Data, including unauthorized or unlawful Processing and Security Incidents.

5.2 You shall promptly respond to changes in legal obligations and known and foreseeable risks to Personal Data. You shall regularly assess the effectiveness of its information security programs and shall adopt a "privacy / security by design" approach to incorporate privacy and data security protections into its products, services, and operations to protect and manage against foreseeable risks to Personal Data.

6. SECURITY INCIDENT NOTICE

6.1 You shall notify Apexon of a known or reasonably suspected Security Incident within 24 hours after it becomes aware of it and shall set out in such notification: (i) the nature of Security Incident and any actions taken (or proposed to be taken) to address or mitigate the adverse effects of the Security Incident; (ii) the likely consequences of the Security Incident; and (iii) the approximate number of individuals potentially affected, geographic residence of the individuals potentially affected (if known), and specific types of Personal Data concerned.

6.2 The Parties will coordinate investigation of the Security Incident. You agree to fully cooperate with Apexon in Apexon's handling of the matter, including without limitation any investigation, providing Apexon with physical access to the facilities and operations affected, facilitating interviews with You's employees and

others involved in the matter, and making available all relevant records, logs, files, and data reporting or other obligations required by Applicable Law, standard, or as otherwise reasonably required by Apexon.

6.3 Remediation. You shall take immediate necessary and appropriate corrective action to remedy the causes of Security Incident at You's expense, with such remedy to include actions necessary to comply with all Data Protection Law and use best efforts to prevent a recurrence of the Security Incident. You will reimburse Apexon for actual costs incurred in responding to and/or mitigating damages from a Security Incident.

6.4 Third Party Notice. Except as may be expressly required by Applicable Law, You agree that it will not inform any third party of any Security Incident without first obtaining Apexon's prior written consent, other than to inform a complainant that the matter has been forwarded to Apexon's legal counsel.

6.5 Public Relations. You shall not make any public statement in relation to the Security Incident without Apexon's prior written consent and shall assist Apexon with Apexon's management of public relations and public statements in relation to the Security Incident.

6.6 Litigation. You agree to cooperate with Apexon in any litigation or other formal action against third parties deemed necessary by Apexon to protect its rights.

6.7 Apexon's decision shall be final and binding under this Section.

7. TRANSFERS OUTSIDE THE TERRITORY

7.1 You shall not transfer Personal Data outside the jurisdiction of applicable country or Process Personal Data from a country other than the applicable country except without prior written consent of Apexon.

7.2 In the event of any change in, or decision of a competent authority under, Data Protection Law, the Parties shall mutually agree in good faith on any amendments or changes to this DPA to continue to enable transfers of Personal Data to be made (or continue to be made) outside the applicable country without breaching the Data Protection Law of such country and the parties shall reasonably agree in good faith on a timeline for ensuring that such amendments or changes become applicable to third parties.

8. DATA SUBJECT RIGHTS

8.1 You shall: (a) assist Apexon by appropriate technical and organisational measures in fulfilling Apexon's obligations regarding a Data Subject's request to exercise any of their rights under Data Protection Law ("**Data Subject Request**") concerning their Personal Data; and (b) immediately notify Apexon in writing of any Data Subject Request that You receives. You shall take action to assist Apexon with a Data Subject Request within ten (10) calendar days. You shall not respond to the Data Subject Request except on the written instructions of Apexon or as required by Data Protection Law, in which case You shall to the extent permitted by any Data Protection Law inform Apexon of that legal requirement before it responds to the Data Subject Request. You will notify Apexon of any Data Subject Requests by emailing with a read receipt legal3@apexon.com with a copy to You's primary business contact within Apexon.

9. ASSISTANCE

9.1 In relation to Processing of Personal Data by You and Your Sub-Processors, You shall, at the written request of Apexon, assist Apexon in ensuring Apexon's compliance with Apexon's obligations under the applicable Data Protection Law.

9.2 You shall make available to Apexon all information necessary to demonstrate compliance with Your obligations under Data Protection Law, this DPA, and the Agreement.

10. AUDITS

10.1 Third Party Assessments. You will evaluate and maintain applicable information technology controls annually by a recognized third-party audit firm based on recognized industry best practices.

10.2 Reports. You will make available to Apexon for review all of the following, as applicable, and upon Apexon's written request: SSAE 18 SOC 1 Type II reports, AT101 SOC 2 Type II reports, and AT101 SOC 3 reports, the latest PCI Compliance Report, and reports relating to ISO certification (as applicable). Apexon agrees to treat such audit reports as confidential information. Any exceptions noted in the report(s) will be addressed in the report with management's corrective action. You also will make available to Apexon all information necessary to demonstrate compliance with the obligations under Data Protection Law, upon Apexon's reasonable request.

10.3 Security Review. Upon request, You will grant Apexon, or a third party on Apexon's behalf, permission to perform an assessment, audit, examination, or review of controls in You's environment in relation to the Personal Data being handled and/or Services being provided to confirm compliance with the Agreement, as well as any Applicable Law, regulations, and industry standards. You will fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that processes, stores, or transports Personal Data for Apexon pursuant to the Agreement.

10.4 Questionnaire. Upon Apexon's written request, You will promptly and accurately complete an information security questionnaire provided by Apexon or a third party on Apexon's behalf regarding You's environment in relation to the Personal Data being handled and/or Services being provided to confirm compliance with the Agreement, as well as any Applicable Law. You will fully cooperate with such inquiry. Apexon will treat the information provided by You in the security questionnaire as confidential.

11. **DELETION OR RETURN OF PERSONAL DATA**

11.1 Upon termination or expiration of the Principal Agreement, at Apexon's option, You shall permanently delete (permanent removal, aggregation, or de-identification consistent with Data Protection Law) or return all Personal Data, including any existing copies thereof in You's possession, unless Applicable Law requires otherwise.

11.2 You shall upon Apexon's reasonable request provide written certification to Apexon's satisfaction that it has fully complied with this Section 111.

12. **GENERAL**

12.1 Material Breach. Your failure to comply with any of the provisions of this DPA is a material breach of this DPA and the Principal Agreement. In such event, Apexon may terminate the Agreement effective immediately upon written notice to You. Apexon shall have no further liability or obligation to You.

12.2 Indemnification. You shall defend, indemnify, and hold harmless Apexon, and its Affiliates, and their respective officers, directors, employees, agents, successors, and permitted assigns (each, a "**Apexon Indemnitee**") from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers, arising out of or resulting from any third party claim against any Apexon Indemnitee arising out of or resulting from (i) any breach by the You of your obligations under Data Protection Law, the Agreement, or this DPA; (ii) You (or any person acting on Your behalf) acting outside or contrary to the instructions of the Apexon in respect of the Processing of Personal Data; (iii) any Security Incidents related to the Processing of Personal Data under this Agreement or DPA.

12.3 Insurance. You shall place and maintain with responsible insurance carriers, policies naming Apexon as an additional insured and amounts of insurance as set forth herein. Upon Apexon's request, You will provide Apexon with a Certificate of Insurance naming Apexon as an additional insured on the appropriate policies and evidencing the coverage as specified herein. All insurance carriers shall waive right of subrogation against Apexon and each insurance policy shall have any applicable "Insured v. Insured" exclusion amended allow Apexon, as the additional insured, to bring a claim against You without invalidating Your coverage under such insurance policy. You shall provide minimum 30 days' notice regarding cancellation of coverage to Apexon.

12.4 In the event of any inconsistency between the terms and/or definitions of this DPA and the Agreement, the terms and/or definitions of this DPA shall prevail.

13. **Additional Obligations:**

13.1 Your information safeguards will include: (a) secure facilities, data centers, paper files, servers, back-up systems and computing equipment including, but not limited to, all mobile devices and other equipment with information storage capability; (b) network, device application, database and platform security; (c) secure transmission, storage and disposal; (d) authentication and access controls within applications, operating systems and equipment; (e) logging all access and exfiltration, and retention of such access control logs for a period of at least one (1) year; (f) encryption of Personal Data at rest including when stored on any electronic notebook, portable hard drive, or removable electronic media with information storage capability; (g) encryption of Personal Data when transmitted over public or wireless networks; (h)

separation of Personal Data from information of Your other customers; (i) personnel security and integrity including, but not limited to, background checks consistent with Applicable Law; (j) annual external and internal penetration testing and quarterly vulnerability scans and promptly implementing, at Your sole cost and expense, a corrective action plan (including timeline) to correct material issues that are identified through testing; and (k) limiting access of Personal Data, and providing privacy and information security training, to Your Authorized Personnel. "**Authorized Personnel**" means Your personnel who have a need to know or otherwise access Personal Data to enable You to perform its obligations under the Agreement, and who are bound in writing by obligations of confidentiality sufficient to protect Personal Data in accordance with the terms of the Agreement and the DPA.

13.2 You will not introduce to Apexon's or any Affiliate's systems or devices, or use any software or code, that contains any virus, malware, ransomware, keylogger, logic bomb, Trojan horse, worm, or other software routines designed to: (a) permit unauthorized access to Apexon's or any Affiliate's systems or devices; (b) disable, erase, or otherwise harm software, hardware, or data owned or controlled by Apexon or any Affiliate; or (c) record or monitor any persons access to Apexon's or any Affiliate's systems or devices.

13.3 You will maintain and implement as necessary a disaster recovery and business continuity plan ("DRBC Plan") which shall include at a minimum: (a) documentation of applicable business processes, procedures and responsibilities; (b) back-up methodology; (c) identification of disaster recovery scenarios and service level agreements for service recovery; (d) responsibilities of Sub-Yous in the event of a disaster; (e) a communications strategy; and (f) procedures for reverting to normal service. The DRBC Plan shall be reviewed annually, or at such other times as may be requested by Apexon. You shall ensure it is able to implement the DRBC Plan at any time in accordance with its terms. You shall test the DRBC Plan on a regular basis (and, in any event, not less than annually). Apexon shall be entitled to participate in such tests as it may reasonably require. Following each test, You shall send to Apexon a written report summarizing the results of the test and shall promptly implement any actions or remedial measures which Apexon reasonably considers to be necessary as a result of those tests.

13.4 You will implement appropriate safeguards to protect Personal Data that are consistent with accepted industry practices (such as ISO 27001 / 27002, ITIL, COBIT or other industry standards of information security), and will ensure that all such safeguards comply with Data Protection Law, the Agreement and the DPA.

Signature of Authorised Signatory

Stephen Samuels

Name of the Organisation / Consultant :

Date :