CUSTOMER DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Schedules and Annexes ("DPA"), forms part of the Agreement (as defined below), by and between Customer and Bigstrum Solutions Private Limited (also referred to herein as a "Party" or collectively as the "Parties"). For the avoidance of doubt, execution of the Agreement shall constitute Customer's signature and acceptance of this DPA and its Schedules, including Annex and Schedule, where applicable.

This DPA between Customer and Bigstrum Solutions Private Limited contains the legal terms and conditions that apply to the Processing of Personal Data by Security Solutions, where Customer is acting as the Controller of Personal Data and Bigstrum Solutions Private Limited is acting as a Processor of Personal Data. Unless otherwise specified in this DPA, the terms of the Agreement shall continue in full force and effect. All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. In the event of any inconsistency between the terms of this DPA and the terms of the Agreement, the terms of this DPA shall prevail.

1. DEFINITIONS

"Affiliates" means, solely for the purposes of this DPA, (i) with respect to Customer, its Affiliates as defined in the Agreement, and (ii) with respect to Bigstrum Solutions Private Limited, entities Controlled by, or under common Control with Bigstrum Solutions Private Limited that Process Personal Data under the direct authority of Bigstrum Solutions Private Limited in order to provide the Security Solutions, where "Control" means having the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise.

"Agreement" means any underlying Bigstrum Solutions Private Limited End User License Agreement, Master Services Agreement, Engagement Letter, Statements of Work, or other legally entered and binding written, or electronic agreement entered into between Bigstrum Solutions Private Limited and Customer that governs the provision of Security Solutions by Bigstrum Solutions Private Limited to Customer.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data

"Data Protection Laws" means all mandatory data protection laws that apply to the Processing of Personal Data under this DPA and the Agreement. Such laws may include, but are not limited to, European Data Protection Law, as defined herein, and U.S. Privacy Laws as defined herein, including the California Consumer Privacy Act, as amended ("CCPA").

"Data Subject" means an identified or identifiable natural person to whom Personal Data relates.

“Personal Data” means any electronic information submitted by or on behalf of Customer to the Security Solutions(s) that (i) relates to an identified or identifiable natural person; and (ii) is defined as "personally identifiable information", "personal information", "personal data" or similar terms under Data Protection Laws.

“Privacy Datasheet(s)” means the applicable document located in Bigstrum Solutions Private Limited Trust Center, that further describes the Processing activities in relation to the Security Solutions provided to Customer under the Agreement.

"Process", "Processes", "Processing", and "Processed" means any operation or set of operations performed upon Personal Data, whether or not by automatic means.

“Processor” means the entity which Processes Personal Data on behalf of the Controller, including as applicable any “service provider” as that term is defined by the CCPA.

“Security Incident” means a breach of security, of which Bigstrum Solutions Private Limited becomes aware, leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data in Bigstrum Solutions Private Limited’ possession, custody, or control that compromises the security, confidentiality, or integrity of such Personal Data.

“Security Measures” means the technical and organizational measures implemented by Bigstrum Solutions Private Limited designed to secure Personal Data, , which are incorporated by reference in Annex II, Schedule 1 of this DPA.

“Security Solution(s)” means, collectively, Bigstrum Solutions Private Limited Products, Support Services, and Unit42 Services purchased by Customer (as such equivalent terms are defined in the applicable Agreement(s) between the Parties), which Process Personal Data.

"Sub-processor" means an entity engaged by Bigstrum Solutions Private Limited to assist in fulfilling its obligations with respect to providing the Security Solution(s) pursuant to the Agreement or this DPA, insofar as such an entity Processes Personal Data on behalf of Bigstrum Solutions Private Limited. For the avoidance of doubt, Bigstrum Solutions Private Limited Affiliates may act as Sub-processors and Process Personal Data on behalf of Bigstrum Solutions Private Limited.

“Trust Center” means the dedicated Bigstrum Solutions Private Limited website that provides customers with comprehensive information, resources and documentation about the company's commitment to data privacy, security, and compliance, found at https://niraapadh.com/legal-notices/trust-center

2. PROCESSING OF PERSONAL DATA

2.1 Scope of Processing. Bigstrum Solutions Private Limited will only Process Personal Data in accordance with Customer's written instructions, the applicable Privacy Datasheets, Data Protection Laws, and this DPA. The Parties agree that this DPA, including all applicable Schedules, the applicable Privacy Datasheets, and the Agreement set out the Customer's written instructions to Bigstrum Solutions Private Limited in relation to the Processing of Personal Data by Bigstrum Solutions Private Limited. Bigstrum Solutions Private Limited shall promptly inform Customer if, in its opinion, any Customer instructions infringe Data Protection Laws.

2.2 Customer Obligations. Customer shall (i) comply with all applicable laws, including Data Protection Laws, in respect of its use of the Security Solution(s); (ii) ensure that any instructions provided to Bigstrum Solutions Private Limited are at all times in accordance with Data Protection Laws; (iii) collect all Personal Data and provide all required notices in accordance with Data Protection Laws and obtain all consents and rights necessary for the Processing of Personal Data; (iv) maintain at all times the accuracy, quality, and legality of Personal Data; and (v) provide to Bigstrum Solutions Private Limited the minimum amount of Personal Data necessary for the provision of the Security Solution(s).

2.3 Confidentiality of Processing. Bigstrum Solutions Private Limited shall ensure that any person who is authorized by Bigstrum Solutions Private Limited to Process Personal Data shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

3. SUB-PROCESSING

3.1 As part of the provision of Security Solution(s), Bigstrum Solutions Private Limited may engage Sub-processors to Process Personal Data on Customer's behalf. Customer hereby grants Bigstrum Solutions Private Limited a general authorization to appoint and use the Sub-processors currently listed on the "List of Sub-processors" which is available in the Trust Center.

3.2 In the event Bigstrum Solutions Private Limited contracts the Processing of Personal Data to a new Sub-processor, Customer will be notified via email in advance of this change, provided Customer has subscribed to receive notifications through the Bigstrum Solutions Private Limited Trust Center, where the List of Sub-processors will be updated. Customer will have thirty (30) calendar days from the date of notification to notify Bigstrum Solutions Private Limited of Customer's objections based on reasonable grounds and only in respect to data protection concerns ("Review Period"). In such cases, Bigstrum Solutions Private Limited will then endeavor to offer alternate options for the delivery of the relevant Security Solution(s) that does not involve the new Sub-processor. The Parties agree that Customer's non-response during the Review Period will be taken as the Customer's approval of such Sub-processor.

3.3 Bigstrum Solutions Private Limited will: (i) enter into a written agreement with all Sub-processors that imposes data protection terms as stringent as those set forth in this DPA; and (ii) remain fully liable for the Sub- processor's compliance with the obligations of this DPA.

3.4 Bigstrum Solutions Private Limited may engage Sub-processors located outside the jurisdiction in which the Personal Data was collected. In such cases, Bigstrum Solutions Private Limited will, where required, implement and maintain an appropriate transfer mechanism to ensure compliance with the Data Protection Laws. This may include, as appropriate, (i) Module 3 of the Standard Contractual Clauses; (ii) an adequacy decision or equivalent issued by the competent regulatory authority; or (iii) or any other mechanism permitted under the Data Protection Laws.

4. COOPERATION

4.1 Government requests for Personal Data. If a law enforcement, national security, or other government agency sends Bigstrum Solutions Private Limited a request (e.g. warrant, court order, or subpoena) to access Personal Data, Bigstrum Solutions Private Limited commits to following the process described here.

4.2 Data Subject requests. In the event of a Personal Data request from a Data Subject related to a Customer is made directly to Bigstrum Solutions Private Limited, Bigstrum Solutions Private Limited shall inform the requestor that Bigstrum Solutions Private Limited is not authorized to directly respond to the request, and recommend the requestor submit the request directly to Customer, unless legally compelled to respond under the law applicable to such a request. Customer shall bear the responsibility for responding to all such requests. In the event Customer requires reasonable support from Bigstrum Solutions Private Limited in responding to a request from a Data Subject, it may contact dpo@bigstrum.in for assistance.

4.3 Data Protection Impact Assessments. Taking into account the nature of the Processing and information available to Bigstrum Solutions Private Limited, Bigstrum Solutions Private Limited shall provide reasonable information regarding the Security Solutions to enable the Customer to carry out data protection impact assessments or similar evaluations and assessments if required by Data Protection Laws.

4.4 Supervisory/Regulatory Authorities. Bigstrum Solutions Private Limited shall provide reasonable assistance to Customer in the cooperation or prior consultations with supervisory authorities or other competent regulatory authorities.

5. SECURITY

5.1 Security Measures. Bigstrum Solutions Private Limited shall implement and maintain the Security Measures.

5.2 Customer Responsibilities. Customer is responsible for secure and appropriate use of the Security Solutions, to ensure a level of security appropriate to the risk in respect of the Personal Data.

5.3 Security Reports. Bigstrum Solutions Private Limited shall make available to Customer, upon written request and without undue delay (subject to appropriate confidentiality obligations), a summary copy of applicable third-party audit report(s) or certifications it maintains for its Security Solutions (e.g. ISO 27001 or SOC2 Type II standard), so that the Customer can verify Bigstrum Solutions Private Limited compliance with this DPA, the audit standards against which it has been assessed, and the standards specified in the Security Measures.

5.4 Security Incidents. Upon confirming that a Security Incident has occurred, without undue delay (no later than seventy-two (72) hours) Bigstrum Solutions Private Limited shall: (i) taking into account the nature of Bigstrum Solutions Private Limited Processing of Personal Data and the information available to Bigstrum Solutions Private Limited, send written notification to the Customer at either the email address listed in Customer's online privacy policy or the email address Customer designates in the Bigstrum Solutions Private Limited Customer Support Portal; and (ii) promptly take such steps as Bigstrum Solutions Private Limited deems necessary and reasonable to contain, investigate, and mitigate the Security Incident to the extent the remediation is within Bigstrum Solutions Private Limited' reasonable control. Bigstrum Solutions Private Limited shall reasonably cooperate with Customer in any post Security Incident communication efforts. The obligations contained herein shall not apply to Security Incidents that are caused by Customer or Customer's users.

6. DELETION AND RETENTION

On termination or expiration of the Agreement, and upon Customer's written request, in accordance with the retention period set forth in the applicable Privacy Datasheet, Bigstrum Solutions Private Limited shall, without undue delay: (i) return a copy of Personal Data to the Customer by secure file transfer in such format as is reasonably requested by the Customer; or (ii) securely delete existing copies of Personal Data, unless continued retention is required and/or permitted by Data Protection Laws and/or mandatory applicable law. If Bigstrum Solutions Private Limited determines that continued retention is required and/or permitted by Data Protection Laws and/or mandatory applicable law, Bigstrum Solutions Private Limited shall ensure the confidentiality of such Personal Data and shall extend the protections of this DPA to such Personal Data.

7. LIMITATION OF LIABILITY

The liability of each party and each party's Affiliates under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement and shall not be modified by this DPA. Any claims brought by a party or its Affiliates under this DPA, whether in contract, tort or under any other theory of liability, shall be subject to the exclusions and limitations set forth in the Agreement, as permitted by applicable law and any claim under this DPA will be aggregated with any claims under the Agreement.

8. JURISDICTION-SPECIFIC SCHEDULES

Attached to this DPA are Schedules that provide terms specific to the Processing of Personal Data arising out of specific legal requirements from particular jurisdictions, which shall apply to the extent Personal Data is Processed in one or more of these jurisdictions. In the event of a conflict or inconsistency between this DPA and a Schedule, the Schedule applicable to Personal Data from the relevant jurisdiction shall prevail with respect to Personal Data from that relevant jurisdiction, but solely with regard to the portion of the provision in conflict or inconsistency. To the extent the Agreement or this DPA contemplates Personal Data transfers from a jurisdiction not included in this DPA, the Parties agree to comply with the relevant jurisdiction's legal requirements.

9. UPDATES TO DPA

In the event of changes to Data Protection Laws, including, but not limited to, the amendment, revision, or introduction of new laws, regulations, or other legally binding requirements to which either party is subject, the Parties agree to revisit the terms of this DPA, and negotiate any appropriate or necessary updates in good faith, including the addition, amendment, or replacement of any Schedules.

SCHEDULE 1

INDIA (DIGITAL PERSONAL DATA PROTECTION ACT, 2023)

1. DEFINITIONS

1.1 “India” means the Republic of India.

1.2 “Indian Data Protection Law” means the Digital Personal Data Protection Act, 2023 (“DPDP Act”), together with any rules, regulations, notifications, or amendments issued thereunder, and any other applicable laws in India governing the processing of digital personal data, including but not limited to the Information Technology Act, 2000 and applicable rules.

1.3 “Data Fiduciary” shall have the meaning assigned under the DPDP Act and corresponds to the “Controller” under this DPA.

1.4 “Data Processor” shall have the meaning assigned under the DPDP Act and corresponds to the “Processor” under this DPA.

1.5 “Data Principal” means the natural person to whom the Personal Data relates, as defined under the DPDP Act.

1.6 “Consent Manager” means an entity registered with the appropriate authority under the DPDP Act to enable Data Principals to give, manage, review, and withdraw consent.

1.7 For the purpose of this Schedule 1, all terms used herein but not defined in the DPA shall have the meaning assigned to them under the applicable Indian Data Protection Law, and all references to Data Protection Law or laws in the DPA shall be read in the context of Indian law.

2. PROCESSING OF PERSONAL DATA UNDER INDIAN LAW

2.1 Lawful Processing

Bigstrum Solutions Private Limited shall process Personal Data only:

On the basis of valid consent obtained by the Customer (Data Fiduciary), or

For legitimate uses as permitted under the DPDP Act

2.2 Purpose Limitation

Processing shall be limited to the purpose specified by the Customer and shall not exceed such purpose.

2.3 Data Minimization

Bigstrum Solutions Private Limited shall process only such Personal Data as is necessary for the provision of the Services.

2.4 Accuracy

Customer shall ensure that Personal Data provided is accurate and complete. Bigstrum shall implement reasonable measures to support data accuracy.

3. CROSS-BORDER DATA TRANSFERS

3.1 Personal Data may be transferred outside India subject to:

Any restrictions or conditions imposed by the Government of India under the DPDP Act

Compliance with applicable notifications regarding restricted jurisdictions

3.2 In the event that any jurisdiction is restricted or prohibited by the Government of India, the Parties shall implement appropriate safeguards or cease such transfers.

3.3 Bigstrum Solutions Private Limited shall ensure that cross-border transfers are conducted with appropriate security and contractual safeguards.

4. OBLIGATIONS OF BIGSTRUM SOLUTIONS PRIVATE LIMITED (DATA PROCESSOR)

Bigstrum Solutions Private Limited shall:

4.1 Process Personal Data only on documented instructions from the Customer.

4.2 Implement appropriate technical and organizational security measures to protect Personal Data.

4.3 Ensure confidentiality obligations for personnel processing Personal Data.

4.4 Assist the Customer in complying with obligations under the DPDP Act, including:

Responding to Data Principal requests

Implementing data protection impact assessments (where applicable)

4.5 Notify the Customer of any Personal Data Breach without undue delay.

4.6 Delete or return Personal Data upon termination of services, unless retention is required by law.

5. PERSONAL DATA BREACH AND INCIDENT RESPONSE

5.1 Bigstrum Solutions Private Limited shall notify the Customer without undue delay upon becoming aware of a Personal Data Breach.

5.2 Bigstrum shall assist the Customer in meeting its obligations under the DPDP Act, including:

Notification to the Data Protection Board of India

Notification to affected Data Principals, where required

5.3 Where applicable, Bigstrum shall support compliance with CERT-In Directions (2022), including incident reporting timelines.

6. DATA PRINCIPAL RIGHTS

6.1 Bigstrum shall assist Customer in enabling Data Principal rights, including:

Right to access information

Right to correction and erasure

Right to grievance redressal

Right to withdraw consent

6.2 Data Subject Access Requests may be directed to:

dsar@bigstrum.in (mailto:dsar@bigstrum.in)

7. SIGNIFICANT DATA FIDUCIARY SUPPORT

Where Customer is classified as a Significant Data Fiduciary under the DPDP Act, Bigstrum shall provide reasonable assistance to support:

Appointment of Data Protection Officer

Conduct of Data Protection Impact Assessments

Periodic audits

8. DATA RETENTION

8.1 Personal Data shall be retained only for as long as necessary to fulfill the purpose of processing or as required by law.

8.2 Upon completion of the purpose or withdrawal of consent, Personal Data shall be deleted unless retention is required under applicable law.

9. GRIEVANCE REDRESSAL AND CONTACT

9.1 Bigstrum shall cooperate with Customer in handling grievances from Data Principals.

9.2 Contact details:

Data Protection Officer: dpo@bigstrum.in (mailto:dpo@bigstrum.in)

Grievance / DSAR: dsar@bigstrum.in (mailto:dsar@bigstrum.in)

10. COMPETENT AUTHORITY

The competent authority under this Schedule shall be:

Data Protection Board of India (upon full operationalization under the DPDP Act)

ANNEX I TO SCHEDULE 1 (INDIA)

A. List of Parties

Data Fiduciary (Controller): Customer

Data Processor: Bigstrum Solutions Private Limited

B. Description of Processing

1. Categories of Data Principals: Employees, customers, partners, contractors
2. Categories of Personal Data: Contact data, system logs, device data, security telemetry
3. Sensitive Personal Data: May be processed depending on service scope
4. Frequency: Continuous
5. Nature: Collection, storage, analysis, transmission, security monitoring
6. Purpose: Cybersecurity, compliance, risk intelligence
7. Retention: As per contractual and legal requirements
8. Sub-processing: As per Trust Center disclosures

C. Competent Authority

Data Protection Board of India

ANNEX II TO SCHEDULE 1

Technical and Organizational Measures

Bigstrum Solutions Private Limited Security Measures can be found at:

https://niraapadh.com/legal-notices/trust-center (https://niraapadh.com/legal-notices/trust-center)

SCHEDULE 2

EUROPEAN ECONOMIC AREA

1. DEFINITIONS

1.1 "EEA" means the European Economic Area.

1.2 "European Data Protection Law" means the 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 ("General Data Protection Regulation" or "GDPR"), as implemented by countries within the EEA and/or other laws that are similar, equivalent to, or successors to the GDPR.

1.3 "Standard Contractual Clauses" means 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.

1.4 For the purpose of this Schedule 1, all terms used herein not defined in the DPA will have the meaning assigned to them in the applicable European Data Protection Law and all references to Data Protection Law or laws in the DPA shall be read in the context of EU or Member State Law.

2. TRANSFERS OUTSIDE OF THE EEA

2.1 Module 2 (Controller to Processor) of the Standard Contractual Clauses. To the extent that Customer, as a Controller, transfers any Personal Data from the EEA for Processing directly to any Bigstrum Solutions Private Limited entity or Affiliate in a third country not deemed by the European Commission to provide an adequate level of data protection, Module 2 (Controller to Processor) of the Standard Contractual Clauses will apply with respect to such transfers.

2.2 Module 3 (Processor to Processor) of the Standard Contractual Clauses. To the extent Bigstrum Solutions Private Limited transfers Personal Data from the EEA for Processing to any Sub-processor in a third country not deemed by the European Commission to provide an adequate level of data protection, Bigstrum Solutions Private Limited shall ensure such transfer is supported by a valid transfer mechanism, which may include use of the Module Three (Processor-to-Processor) of the Standard Contractual Clauses.

2.3 Where available, Bigstrum Solutions Private Limited will rely on existing adequacy decisions approved by the European Commission. In the event such adequacy decision is not available, or in the event of any change in Data Protection Laws or binding legal decision by the relevant judicial or competent authority renders an existing adequacy decision invalid or insufficient to support the transfer of Personal Data outside the of the EEA, Bigstrum Solutions Private Limited will rely on Standard Contractual Clauses as the legally valid data transfer mechanism. To the extent the execution of additional documents is required to give effect to such data transfer solution, the Parties shall work in good faith to execute such documentation.

3. STANDARD CONTRACTUAL CLAUSES

3.1 To the extent applicable under Clause 2.1 of this Schedule 1, Module Two (Controller to Processor) of the Standard Contractual Clauses is incorporated by reference into this Schedule 1. For clarity, Annexes I and II of the Standard Contractual Clauses are attached to this Schedule 1. Signatures applied to the Agreement will be taken as equally signing and effectuating the Standard Contractual Clauses.

3.2 In respect to Clause 7 Docking clause, the option shall not apply.

3.3 In respect to Clause 9(a) Sub-processors, option 2 is selected and Customer grants a General Written Authorization for the use of Sub-processors listed here. All other provisions contained in Clause 3 of this Schedule 1 shall apply.

3.4 In respect to Clause 11 Redress, the option shall not apply.

3.5 In respect to Clause 17 Governing Law, option 1 is selected and the governing law is that of The Netherlands.

3.6 In respect to Clause 18 Choice of forum and jurisdiction, the courts of The Netherlands shall resolve any disputes arising from the Standard Contractual Clauses.

ANNEX I TO SCHEDULE 2

A. List of Parties

Data exporter: The data exporter is the entity identified as the Customer in the Agreement, acting as a data exporter on behalf of itself and its Affiliates.

Data importer: The data importer is Bigstrum Solutions Private Limited.

B. Description of Transfer

1. Categories of Data Subjects whose personal data is transferred: The Personal Data transferred may relate to the following categories of Data Subjects: Employees, contractors, consultants, individuals belonging to Customer, Customer's clients', and partners' workforce and/or other individuals whose Personal Data is Processed as part of the provision of the Security Solutions .

2. Categories of personal data transferred: The Personal Data transferred may relate to the following categories of Personal Data: a) Identification and contact data (e.g., name, address, phone number, title, email, other contact details); b) Employment details (e.g., job title, role, manager); c) IT information (e.g., entitlements, IP addresses, usage data, cookies data, online identifiers); d) Domain and device information (e.g., MAC address, hostnames, International

Mobile Subscriber Identity (IMSI), International Mobile Equipment Identity (IMEI), and qualified hostnames); e) Information contained in logs related to security events identified and captured by Security Solution(s); and/or f) Unstructured data provided to Bigstrum Solutions Private Limited for the purpose of providing services (e.g., packet capture (PCAP) for file testing).

For the specific categories of Personal Data Processed on a Security Solution per Security Solution basis, refer to the applicable Privacy Datasheets available at the Trust Center.

3. Sensitive data transferred (if applicable): When Processing Personal Data, primarily with forensic investigations Security Solution(s) of which the purpose is to identify the underlying data, Bigstrum Solutions Private Limited may process sensitive Personal Data. The nature and scope of the sensitive personal data that is transferred may not be known until after the Processing has taken place and may include: Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

4. The frequency of the transfer (e.g., Whether the data is transferred on a one-off or continuous basis): The transfer of Personal Data between the Parties will occur on a continuous basis.

5. Nature of the Processing: Personal Data will be subject to processing activities such as storing, recording, using, sharing, transmitting, analyzing, collecting, transferring, and making available Personal Data. Additional details regarding Bigstrum Solutions Private Limited' Processing activities are reflected in the applicable Privacy Datasheets, available at the Trust Center.

6. Purpose: The purpose of the Processing of Personal Data under this DPA is to enable Bigstrum Solutions Private Limited to deliver the Security Solution(s) (s) and perform its obligations as set forth in the Agreement (including this DPA) or as otherwise agreed by the Parties in mutually executed written form. For specific details on Bigstrum Solutions Private Limited purposes for Processing Personal Data under a specific Security Solution(s) , please refer to the applicable Privacy Datasheets available at the Trust Center.

7. The period for which the personal data will be retained, or if that's not possible, the criteria used to determine that period: Bigstrum Solutions Private Limited will retain Personal Data to fulfill the purposes for which it was collected and as necessary to comply with business requirements, legal obligations, resolve disputes, and enforce its rights. Specific data retention periods are listed for certain Security Solution(s) in the applicable Privacy Datasheets available at the

Trust Center.

8. For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing: Personal Data will be transferred to Bigstrum Solutions Private Limited Sub-processors as described in the applicable Privacy Datasheet available at the Trust Center.

C. Competent Supervisory Authority

Competent supervisory authority/ies to be chosen in accordance with Clause 13.

ANNEX II TO SCHEDULE 2

Technical and Organizational Measures

Bigstrum Solutions Private Limited Security Measures can be found at:

https://niraapadh.com/legal-notices/trust-center (https://niraapadh.com/legal-notices/trust-center)

SCHEDULE 3

UNITED KINGDOM

1. DEFINITIONS

1.1 "Mandatory Clauses" means Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before Parliament in accordance with s199A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

1.2 "Standard Contractual Clauses" means 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.

1.3 "UK" means the United Kingdom.

1.4 "UK Data Protection Law" means all laws relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in the UK, including: (i) the UK GDPR and UK Data Protection Act 2018; and/or (ii) other laws that are similar, equivalent to, successors to, or that are intended to or implement the laws that are identified in (i) above.

1.5 "UK GDPR" as defined in Section 3 of the Data Protection Act 2018.

1.6 For the purposes of this Schedule 2, all terms used herein not defined in the DPA will have the meaning assigned to them in the applicable UK Data Protection Law and all references to Data Protection Law or laws in the DPA shall be read in the context of UK Law.

2. TRANSFERS OUTSIDE OF THE UK

2.1 To the extent that Customer transfers any Personal Data from the UK for Processing directly to any Bigstrum Solutions Private Limited entity or Affiliate in countries not deemed to provide an adequate level of data protection under UK Data Protection Law, the Parties agree to enter into and comply with Module 2 of the Standard Contractual Clauses (as amended by the Mandatory Clauses) and having selected the options identified in Clauses 3.2 - 3.6 of Schedule 1 above. Bigstrum Solutions Private Limited agrees that it is a "data importer" and Customer is the "data exporter" under the Standard Contractual (as amended by the Mandatory Clauses).

2.2 In the event of any change in UK Data Protection Law or binding legal decision by the relevant judicial authority that renders the data transfer mechanism described in Clause 2.1 of this Schedule 2 invalid or insufficient to support the transfer of Personal Data, and to the extent that Bigstrum Solutions Private Limited adopts an available alternative data transfer solution for the lawful transfer of Personal Data outside of the UK (as recognized under UK Data Protection Law) such as the UK Extension to the EU-U.S. Data Privacy Framework, the Parties agree that such transfer will be made in reliance on such alternative data transfer solution. To the extent the

execution of additional documents is required to give effect to such data transfer solution, the Parties shall work in good faith to execute such documentation.

3. MANDATORY CLAUSES

3.1 To the extent applicable under Clause 2.1 of this Schedule 2, Module Two (Controller to Processor) of the Standard Contractual Clauses and the Mandatory Clauses are incorporated by reference into this Schedule 2, and the Standard Contractual Clauses are amended in accordance with the Mandatory Clauses. For clarity, Annexes I and II of the Standard Contractual Clauses included in Schedule 1 are incorporated by reference to this Schedule

2. Signatures applied to the Agreement will be taken as equally signing and effectuating the Approved Addendum, including the Mandatory Clauses.

3.2 Neither the Mandatory Clauses or this Schedule 1 shall be interpreted in a way that conflicts with rights and obligations provided for under UK Data Protection Law.

3.3 Data importer may end this DPA (including this Schedule 2) to the extent the Mandatory Clauses apply, in accordance with Clause 19 of the Mandatory Clauses.

SCHEDULE 4

SWITZERLAND

1. DEFINITIONS

1.1 "FDIP" means the Federal Data Protection and Information Commissioner.

1.2 "GDPR" or "General Data Protection Regulation" means the EU General Data Protection 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.

1.3 "Swiss FADP" means the Swiss Federal Act of 19 June 1992 on Data Protection, the Ordinance to the Swiss Federal Act on Data Protection and the revised Swiss Federal Act of 25 September 2020 on Data Protection which comes into force in 2023.

1.4. For the purpose of this Schedule 3, all terms used herein not defined in the DPA will have the meaning assigned to them in the applicable Swiss FADP and all references to Data Protection Law or laws in the DPA shall be read in the context of the Swiss FADP.

2. TRANSFERS OUTSIDE OF SWITZERLAND

2.1 To the extent that Customer transfers any Personal Data from Switzerland for Processing directly to any Bigstrum Solutions Private Limited entity or Affiliate in a third country not deemed to provide an adequate level of data protection under the Swiss FADP, Module 2 (Controller to Processor) of the Standard Contractual Clauses will apply with respect to such transfers.

2.2 In the event of any change in the Swiss FADP or binding legal decision by the relevant judicial authority that renders the data transfer solution identified in Clause 2.1 of this Schedule 3 invalid or insufficient to support the transfer of Personal Data, and to the extent that Bigstrum Solutions Private Limited adopts an available alternative data export solution for the lawful transfer of Personal Data outside of Switzerland (as recognized under the Swiss FADP) such as the Swiss-U.S. Data Privacy Framework, the Parties agree that such transfer will be made in reliance on such alternative data transfer solution. To the extent the execution of additional documents is required to give effect to such data transfer solution, the Parties shall work in good faith to execute such documentation.

3. STANDARD CONTRACTUAL CLAUSES

3.1. To the extent applicable under Clause 2.1 of this Schedule 3, Module Two (Controller to Processor) of the Standard Contractual Clauses is incorporated by reference into this Schedule 3. Annexes I and II, as set forth in Schedule 1, shall form the Annexes to the Standard Contractual Clauses incorporated in this Schedule 3. Signatures applied to the Agreement will be taken as equally signing and effectuating the Standard Contractual Clauses.

3.2 References to General Data Protection Regulation and/ or GDPR shall be deemed to refer to the Swiss FADP.

3.3 All references to the competent supervisory authority shall be deemed to refer to the Federal Data Protection and Information Commissioner ("FDPIC).

3.4 References to the "European Union", "Union", "EU", and "Member State(s)/EU Member State(s)" shall be deemed to include Switzerland and references to the exporter in the EU shall be deemed to include the exporter in Switzerland.

3.5 Where the Standard Contractual Clauses use terms that are defined in the GDPR, those terms shall be deemed to have the meaning as the equivalent terms are defined in the Swiss FADP.

3.6 In respect to Clause 17 Governing law, the applicable law shall be Swiss law.

3.7 In respect to Clause 18 Choice of forum and jurisdiction, the Swiss courts shall resolve any disputes arising from the Standard Contractual Clauses.

SCHEDULE 5

U.S. PRIVACY LAWS

1. DEFINITIONS

1.1 "U.S. Privacy Laws" means all laws relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in the U.S., including the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act, and its implementing regulations.

1.2 ."Business" or "business" means Customer, a for-profit legal entity that collects consumers' personal information (or has another entity collect consumers' personal information on its behalf) and determines the purposes and means of the Processing of Personal Data.

1.3 For the purpose of this Schedule 4, all terms used herein not defined in this Schedule 4 will have the meaning assigned to them in the U.S. Privacy Laws, its implementing regulations or the Agreement and all references to Data Protection Law or laws in the DPA shall be read in the context of U.S. Privacy Laws.

2. COMMITMENTS UNDER U.S. PRIVACY LAWS

2.1 Bigstrum Solutions Private Limited agrees that:

2.1.1 It is acting solely as a "Service Provider" or "Processor" as defined under the U.S. Privacy Laws;

2.1.2 It will comply with, and provide at least the same level of privacy protection as is required under the U.S. Privacy Laws;

2.1.3 It will notify the business promptly after making the relevant determination if it determines that it can no longer meet its obligations under the U.S. Privacy Laws;

2.1.4 Customer will have the right to take reasonable and appropriate steps to (i) ensure that Bigstrum Solutions Private Limited uses Personal Data in a manner consistent with Customer's obligations under the U.S. Privacy Laws; and (ii) upon reasonable notice, stop and remediate the unauthorized Processing of Personal Data by Bigstrum Solutions Private Limited.

2.1.5 To the extent Bigstrum Solutions Private Limited receives Personal Data in deidentified form from the Customer or deidentifies Personal Data received from Customer such that it cannot reasonably be linked to such Personal Data, directly or indirectly ("Deidentified Data"), Bigstrum Solutions Private Limited will (1) take reasonable measures to ensure that the Deidentified Data cannot be associated with a consumer or household; (2) publicly commit to maintain and use the Deidentified Data in a de-identified form and not attempt to re-identify the information (except that Bigstrum Solutions Private Limited may attempt to re-identify the data solely for the purpose

of determining whether its deidentification processes are compliant with U.S. Privacy Laws); and (3) contractually obligate any recipients of the Deidentified Data to comply with the foregoing requirements and US Privacy Laws.

2.1.6 For the avoidance of doubt, Bigstrum Solutions Private Limited is permitted to deidentify Personal Data through a reliable state of the art anonymization procedure and use such Deidentified Data for its own business purposes, including without limitation for security and fraud detection and research and development of new products and services, provided such Deidentified Data cannot reasonably be linked to the Personal Data, directly or indirectly.

2.2 Except as otherwise permitted by the U.S. Privacy Laws, this DPA or the Agreement, Bigstrum Solutions Private Limited shall not:

2.2.1 retain, use or disclose Personal Data outside of its direct business relationship with Customer or retain, use or disclose Personal Data for any purposes other than the business purposes specified in this DPA or the Agreement;

2.2.2 combine Personal Data of consumers that Bigstrum Solutions Private Limited receives from, or on behalf of, Customer with Personal Data that Bigstrum Solutions Private Limited receives from, or on behalf of, another person or persons or collects from its own interaction with consumers for cross-context behavioral advertising; and

2.2.3 sell or share Personal Data, as those terms are defined by the U.S. Privacy Laws.

SCHEDULE 6

BAHRAIN (PERSONAL DATA PROTECTION LAW)

1. DEFINITIONS

1.1 “Bahrain PDPL” means the Kingdom of Bahrain Personal Data Protection Law (Law No. 30 of 2018), together with its implementing regulations, resolutions, guidance, and any amendments thereto.

1.2 “Controller” means Customer, being the natural or legal person that determines the purposes and means of Processing Personal Data under the Bahrain PDPL.

1.3 “Processor” means Bigstrum Solutions Private Limited, being the entity that Processes Personal Data on behalf of the Controller.

1.4 “Data Subject” means an identified or identifiable natural person to whom Personal Data relates, as defined under the Bahrain PDPL.

1.5 “Personal Data”, “Processing”, and other related terms shall have the meanings assigned to them under the Bahrain PDPL.

1.6 For the purpose of this Schedule 6, all terms used herein not defined in this Schedule 6 shall have the meaning assigned to them under the Bahrain PDPL and its implementing regulations, and all references to Data Protection Law or laws in the DPA shall be read in the context of Bahrain law.

2. COMMITMENTS UNDER BAHRAIN PDPL

2.1 Bigstrum Solutions Private Limited agrees that:

2.1.1 It is acting solely as a Processor on behalf of the Controller under the Bahrain PDPL;

2.1.2 It shall Process Personal Data only on documented instructions from the Controller, unless otherwise required by applicable law;

2.1.3 It shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including protection against unauthorized or unlawful Processing and against accidental loss, destruction, or damage;

2.1.4 It shall ensure that persons authorized to Process Personal Data are subject to confidentiality obligations;

2.1.5 It shall assist the Controller in complying with its obligations under the Bahrain PDPL, including:

Responding to Data Subject rights requests

Ensuring security of Processing

Supporting breach notification obligations

2.1.6 It shall notify the Controller without undue delay upon becoming aware that it can no longer meet its obligations under the Bahrain PDPL;

2.1.7 The Controller shall have the right to take reasonable and appropriate steps to:

(i) Ensure that Bigstrum Solutions Private Limited Processes Personal Data in a manner consistent with the Controller's obligations under the Bahrain PDPL; and

(ii) Upon reasonable notice, stop and remediate any unauthorized Processing of Personal Data.

3. DATA SUBJECT RIGHTS

3.1 Bigstrum Solutions Private Limited shall assist the Controller in enabling Data Subject rights under the Bahrain PDPL, including:

Right to access Personal Data

Right to rectification

Right to object to Processing

Right to erasure (where applicable)

3.2 Data Subject requests may be directed to:

dsar@bigstrum.in(mailto:dsar@bigstrum.in)

4. DATA TRANSFERS OUTSIDE BAHRAIN

4.1 Personal Data shall not be transferred outside the Kingdom of Bahrain unless:

The destination country provides an adequate level of protection as determined by the competent authority; or

Appropriate safeguards are implemented in accordance with the Bahrain PDPL; or

Such transfer is otherwise permitted under applicable law

4.2 Bigstrum Solutions Private Limited shall ensure that any cross-border transfers are subject to appropriate contractual and technical safeguards.

5. PERSONAL DATA BREACH

5.1 Bigstrum Solutions Private Limited shall notify the Controller without undue delay upon becoming aware of a Personal Data Breach.

5.2 Bigstrum shall provide reasonable assistance to enable the Controller to comply with its breach notification obligations under the Bahrain PDPL.

6. SUB-PROCESSING

6.1 Bigstrum Solutions Private Limited may engage Sub-processors subject to:

Prior authorization from the Controller (general or specific)

Imposition of equivalent data protection obligations

6.2 Bigstrum shall remain fully liable for the performance of its Sub-processors.

7. DATA RETENTION AND DELETION

7.1 Personal Data shall be retained only for as long as necessary to fulfill the purposes for which it was collected or as required under applicable law.

7.2 Upon termination of the Agreement, Bigstrum Solutions Private Limited shall, at the Controller's choice:

Return Personal Data; or

Securely delete Personal Data

unless retention is required by law.

8. RESTRICTIONS ON PROCESSING

8.1 Except as otherwise permitted under the Bahrain PDPL, this DPA, or the Agreement, Bigstrum Solutions Private Limited shall not:

8.1.1 Retain, use, or disclose Personal Data for any purpose other than as necessary to perform the Services or as required by law;

8.1.2 Process Personal Data in a manner inconsistent with the Controller's instructions;

8.1.3 Disclose Personal Data to third parties except as authorized under this DPA or required by law.

9. COMPETENT AUTHORITY

9.1 The competent supervisory authority under this Schedule shall be:

Personal Data Protection Authority (Kingdom of Bahrain)

Below are contract-ready Schedules for UAE, Saudi Arabia, and Qatar, drafted in the same structure, tone, and legal rigor as your U.S. and Bahrain schedules. These are fully aligned for integration into your global DPA.

SCHEDULE 7

UNITED ARAB EMIRATES (PERSONAL DATA PROTECTION LAW)

1. DEFINITIONS

1.1 “UAE PDPL” means the United Arab Emirates Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data, together with its implementing regulations, executive decisions, guidance, and any amendments thereto.

1.2 “Controller” means Customer, being the natural or legal person that determines the purposes and means of Processing Personal Data under the UAE PDPL.

1.3 “Processor” means Bigstrum Solutions Private Limited, being the entity that Processes Personal Data on behalf of the Controller.

1.4 “Data Subject” means an identified or identifiable natural person to whom Personal Data relates, as defined under the UAE PDPL.

1.5 “Personal Data”, “Processing”, and related terms shall have the meanings assigned under the UAE PDPL.

1.6 For the purpose of this Schedule 7, all terms used herein not defined in this Schedule shall have the meaning assigned under the UAE PDPL, and all references to Data Protection Law or laws in the DPA shall be read in the context of UAE law.

2. COMMITMENTS UNDER UAE PDPL

2.1 Bigstrum Solutions Private Limited agrees that:

2.1.1 It is acting solely as a Processor on behalf of the Controller;

2.1.2 It shall Process Personal Data only on documented instructions from the Controller, unless required by applicable law;

2.1.3 It shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk;

2.1.4 It shall ensure confidentiality of personnel authorized to Process Personal Data;

2.1.5 It shall assist the Controller in complying with its obligations under the UAE PDPL, including:

Data Subject rights

Security obligations

Regulatory compliance

2.1.6 It shall notify the Controller without undue delay if it determines that it can no longer meet its obligations under the UAE PDPL;

2.1.7 The Controller shall have the right to take reasonable and appropriate steps to:

(i) Ensure compliance with UAE PDPL; and

(ii) Stop and remediate unauthorized Processing.

3. DATA SUBJECT RIGHTS

3.1 Bigstrum Solutions Private Limited shall assist the Controller in enabling Data Subject rights, including:

Right to access

Right to rectification

Right to erasure

Right to restriction of Processing

3.2 Requests may be directed to:

dsar@bigstrum.in (mailto:dsar@bigstrum.in)

4. DATA TRANSFERS OUTSIDE UAE

4.1 Personal Data shall not be transferred outside UAE unless:

The destination country ensures adequate protection; or

Appropriate safeguards are implemented; or

Transfer is otherwise permitted under UAE PDPL

4.2 Bigstrum shall ensure appropriate contractual and technical safeguards.

5. PERSONAL DATA BREACH

5.1 Bigstrum shall notify the Controller without undue delay upon becoming aware of a Personal Data Breach.

5.2 Bigstrum shall assist in regulatory notification and mitigation.

6. SUB-PROCESSING

6.1 Sub-processors may be engaged subject to:

Authorization from Controller

Equivalent contractual obligations

6.2 Bigstrum remains liable for Sub-processors.

7. DATA RETENTION AND DELETION

7.1 Data shall be retained only as necessary.

7.2 Upon termination:

Return or delete Personal Data

8. RESTRICTIONS ON PROCESSING

8.1 Bigstrum shall not:

Use Personal Data beyond agreed purposes

Disclose without authorization

Process inconsistently with instructions

9. COMPETENT AUTHORITY

UAE Data Office

SCHEDULE 8

SAUDI ARABIA (PERSONAL DATA PROTECTION LAW)

1. DEFINITIONS

1.1 “Saudi PDPL” means the Kingdom of Saudi Arabia Personal Data Protection Law issued by Royal Decree No. M/19 (2021), together with implementing regulations and amendments.

1.2 “Controller” means Customer.

1.3 “Processor” means Bigstrum Solutions Private Limited.

1.4 “Data Subject” means an identifiable natural person.

1.5 Terms shall have meanings assigned under Saudi PDPL.

1.6 All references shall be interpreted in context of Saudi law.

2. COMMITMENTS UNDER SAUDI PDPL

2.1 Bigstrum agrees that:

2.1.1 It acts solely as Processor;

2.1.2 Processes data only per instructions;

2.1.3 Implements security measures;

2.1.4 Maintains confidentiality;

2.1.5 Assists Controller with:

Data Subject rights

Regulatory compliance

2.1.6 Notifies inability to comply;

2.1.7 Allows Controller oversight and remediation rights.

3. DATA SUBJECT RIGHTS

Includes:

Access

Correction

Destruction

Requests:

dsar@bigstrum.in (mailto:dsar@bigstrum.in)

4. DATA TRANSFERS OUTSIDE SAUDI ARABIA

4.1 Transfers allowed only if:

Approved by competent authority; or

Necessary and lawful

4.2 Safeguards must be implemented.

5. PERSONAL DATA BREACH

5.1 Notification without undue delay.

5.2 Assistance in compliance.

6. SUB-PROCESSING

Same obligations as Processor.

7. DATA RETENTION AND DELETION

Retain only as necessary.

8. RESTRICTIONS ON PROCESSING

No unauthorized use, disclosure, or deviation.

9. COMPETENT AUTHORITY

Saudi Data & Artificial Intelligence Authority (SDAIA)

SCHEDULE 9

QATAR (PERSONAL DATA PRIVACY PROTECTION LAW)

1. DEFINITIONS

1.1 “Qatar Data Protection Law” means Law No. 13 of 2016 on Personal Data Privacy Protection and its implementing regulations.

1.2 “Controller” means Customer.

1.3 “Processor” means Bigstrum Solutions Private Limited.

1.4 “Data Subject” means an identifiable individual.

1.5 Terms shall have meanings assigned under Qatar law.

1.6 All references shall be interpreted under Qatar law.

2. COMMITMENTS UNDER QATAR LAW

2.1 Bigstrum agrees that:

2.1.1 It acts solely as Processor;

2.1.2 Processes data per instructions;

2.1.3 Implements security measures;

2.1.4 Ensures confidentiality;

2.1.5 Assists Controller in compliance;

2.1.6 Notifies inability to comply;

2.1.7 Allows oversight and remediation.

3. DATA SUBJECT RIGHTS

Includes:

Access

Correction

Objection

Requests:

dsar@bigstrum.in (mailto:dsar@bigstrum.in)

4. DATA TRANSFERS OUTSIDE QATAR

4.1 Allowed if:

Adequate protection exists; or

Approval obtained

4.2 Safeguards required.

5. PERSONAL DATA BREACH

Notification without delay.

6. SUB-PROCESSING

Allowed with safeguards and authorization.

7. DATA RETENTION AND DELETION

Limited retention obligation.

8. RESTRICTIONS ON PROCESSING

No unauthorized use or disclosure.

9. COMPETENT AUTHORITY

Ministry of Communications and Information Technology (MCIT), Qatar

SCHEDULE 10

BRAZIL (LEI GERAL DE PROTEÇÃO DE DADOS – LGPD)

1. DEFINITIONS

1.1 “Brazil” means the Federative Republic of Brazil.

1.2 “Brazilian Data Protection Law” or “LGPD” means Law No. 13,709/2018 (Lei Geral de Proteção de Dados Pessoais), as amended by Law No. 13,853/2019, together with its implementing regulations, guidelines, and decisions issued by the competent authority.

1.3 “ANPD” means the Autoridade Nacional de Proteção de Dados (Brazilian National Data Protection Authority).

1.4 “Controller” (“Controlador”) means Customer, being the entity responsible for decisions regarding the Processing of Personal Data.

1.5 “Processor” (“Operador”) means Bigstrum Solutions Private Limited, being the entity that Processes Personal Data on behalf of the Controller.

1.6 “Data Subject” (“Titular”) means a natural person to whom the Personal Data relates.

1.7 “Personal Data”, “Sensitive Personal Data”, and “Processing” shall have the meanings assigned under the LGPD.

1.8 For the purpose of this Schedule 10, all terms used herein not defined in the DPA shall have the meaning assigned to them under the LGPD, and all references to Data Protection Law or laws in the DPA shall be read in the context of Brazilian law.

2. INTERNATIONAL TRANSFERS OF PERSONAL DATA

2.1 Transfers Outside Brazil

To the extent that Customer, as Controller, transfers Personal Data from Brazil to Bigstrum Solutions Private Limited in a country that does not provide an adequate level of data protection as determined by the ANPD, such transfer shall be supported by appropriate safeguards in accordance with the LGPD.

2.2 Appropriate Safeguards

Such safeguards may include:

Standard contractual clauses approved or recognized by the ANPD

Contractual provisions ensuring compliance with LGPD principles

Other legally valid mechanisms under Brazilian law

2.3 Sub-processor Transfers

To the extent Bigstrum transfers Personal Data to Sub-processors outside Brazil, Bigstrum shall ensure that such transfers are supported by valid transfer mechanisms and equivalent data protection obligations.

2.4 Adequacy Decisions

Where available, Bigstrum shall rely on adequacy decisions recognized by the ANPD. Where such adequacy decisions are not available, Bigstrum shall implement alternative lawful safeguards.

2.5 Cooperation

The Parties shall cooperate in good faith to implement any additional documentation required to ensure lawful cross-border transfers.

3. CONTRACTUAL SAFEGUARDS

3.1 To the extent required under the LGPD, contractual clauses ensuring data protection obligations are incorporated by reference into this Schedule.

3.2 Such clauses shall ensure:

Compliance with LGPD principles

Data Subject rights protection

Security and confidentiality obligations

3.3 Execution of the Agreement shall constitute acceptance of such contractual safeguards.

4. PROCESSING OBLIGATIONS

4.1 Bigstrum Solutions Private Limited shall:

4.1.1 Process Personal Data only on documented instructions from the Controller;

4.1.2 Ensure compliance with LGPD principles, including:

Purpose limitation

Adequacy

Necessity

Free access

Data quality

Transparency

Security

Prevention

Non-discrimination

Accountability

4.1.3 Implement appropriate technical and organizational measures;

4.1.4 Ensure confidentiality obligations for personnel;

4.1.5 Assist the Controller in fulfilling its obligations under the LGPD;

4.1.6 Notify the Controller if it determines it can no longer meet its obligations.

5. DATA SUBJECT RIGHTS

5.1 Bigstrum Solutions Private Limited shall assist the Controller in enabling Data Subject rights under the LGPD, including:

Confirmation of processing

Access to Personal Data

Correction of incomplete or inaccurate data

Anonymization, blocking, or deletion

Data portability

Information about data sharing

Revocation of consent

5.2 Requests may be directed to:

dsar@bigstrum.in (mailto:dsar@bigstrum.in)

6. PERSONAL DATA BREACH

6.1 Bigstrum Solutions Private Limited shall notify the Controller without undue delay upon becoming aware of a Personal Data Breach.

6.2 Bigstrum shall assist the Controller in complying with obligations to notify:

The ANPD

Affected Data Subjects

6.3 Notifications shall include relevant information regarding:

Nature of the breach

Affected data categories

Mitigation measures

7. SUB-PROCESSING

7.1 Bigstrum may engage Sub-processors subject to:

Authorization from the Controller

Equivalent contractual obligations

7.2 Bigstrum shall remain liable for Sub-processors.

8. DATA RETENTION AND DELETION

8.1 Personal Data shall be retained only as necessary to fulfill processing purposes or comply with legal obligations.

8.2 Upon termination, Bigstrum shall:

Return Personal Data; or

Securely delete Personal Data

unless retention is required by law.

9. RESTRICTIONS ON PROCESSING

9.1 Except as otherwise permitted under the LGPD, this DPA, or the Agreement, Bigstrum Solutions Private Limited shall not:

9.1.1 Retain, use, or disclose Personal Data outside the scope of the Agreement;

9.1.2 Process Personal Data for purposes inconsistent with Controller instructions;

9.1.3 Disclose Personal Data to unauthorized third parties.

10. GOVERNING LAW AND JURISDICTION

10.1 This Schedule shall be governed by the laws of Brazil.

10.2 Any disputes arising under this Schedule shall be subject to the jurisdiction of the competent courts of Brazil.

ANNEX I TO SCHEDULE 10

A. LIST OF PARTIES

Data Exporter (Controller): Customer

Data Importer (Processor): Bigstrum Solutions Private Limited

B. DESCRIPTION OF TRANSFER

1. Categories of Data Subjects: Employees, customers, partners, contractors

2. Categories of Personal Data:

Identification and contact data

Employment data

IT and system data

Security logs and telemetry

Device and network identifiers

3. Sensitive Personal Data:

May include data revealing racial or ethnic origin, health data, biometric data, or other sensitive categories depending on processing scope.

4. Frequency: Continuous

5. Nature of Processing:

Collection, storage, analysis, monitoring, transmission, and security processing

6. Purpose:

Cybersecurity, compliance monitoring, risk intelligence, and service delivery

7. Retention:

As required for service delivery, legal compliance, and contractual obligations

8. Sub-processing:

As described in Trust Center:

https://niraapadh.com/legal-notices/trust-center (https://niraapadh.com/legal-notices/trust-center)

C. COMPETENT AUTHORITY

Autoridade Nacional de Proteção de Dados (ANPD)

ANNEX II TO SCHEDULE 10

Technical and Organizational Measures

Bigstrum Solutions Private Limited Security Measures are available at:

https://niraapadh.com/legal-notices/trust-center (https://niraapadh.com/legal-notices/trust-center)

SCHEDULE 11

SINGAPORE (PERSONAL DATA PROTECTION ACT)

1. DEFINITIONS

1.1 "Singapore PDPA" means the Personal Data Protection Act 2012 (No. 26 of 2012), together with its amendments, regulations, and guidelines issued by the Personal Data Protection Commission ("PDPC").

1.2 "Organization" means Customer, being the entity that determines the purposes and means of Processing Personal Data.

1.3 "Data Intermediary" means Bigstrum Solutions Private Limited, being the entity that Processes Personal Data on behalf of the Organization.

1.4 "Individual" means a natural person to whom Personal Data relates.

1.5 "Personal Data" and "Processing" shall have the meanings assigned under the Singapore PDPA.

1.6 For the purpose of this Schedule 11, all terms not defined herein shall have the meanings assigned under the Singapore PDPA and all references to Data Protection Laws shall be read in the context of Singapore law.

2. TRANSFERS OUTSIDE SINGAPORE

2.1 Personal Data may be transferred outside Singapore only where:

The receiving party is bound by legally enforceable obligations to provide a standard of protection comparable to the PDPA; or

The transfer is otherwise permitted under the Singapore PDPA

2.2 Bigstrum Solutions Private Limited shall ensure:

Appropriate contractual safeguards

Equivalent protection standards

2.3 The Parties shall cooperate to implement additional safeguards if required.

3. CONTRACTUAL SAFEGUARDS

3.1 This DPA incorporates contractual measures ensuring:

Compliance with PDPA obligations

Protection of Personal Data

Accountability and governance

3.2 Execution of the Agreement constitutes acceptance of these safeguards.

4. PROCESSING OBLIGATIONS

4.1 Bigstrum shall:

4.1.1 Process Personal Data only on documented instructions;

4.1.2 Comply with PDPA obligations applicable to Data Intermediaries;

4.1.3 Implement reasonable security arrangements;

4.1.4 Ensure confidentiality;

4.1.5 Assist Customer in meeting its obligations.

5. DATA SUBJECT RIGHTS

5.1 Bigstrum shall assist Customer in responding to:

Access requests

Correction requests

5.2 Requests may be directed to:

dsar@bigstrum.in (mailto:dsar@bigstrum.in)

6. PERSONAL DATA BREACH

6.1 Bigstrum shall notify Customer without undue delay.

6.2 Bigstrum shall assist with notification obligations to:

PDPC

Affected individuals

7. SUB-PROCESSING

7.1 Sub-processors may be engaged with equivalent obligations.

7.2 Bigstrum remains liable.

8. DATA RETENTION AND DELETION

8.1 Retention limited to purpose and legal requirements.

8.2 Return or deletion upon termination.

9. RESTRICTIONS ON PROCESSING

9.1 No unauthorized use, disclosure, or deviation.

10. GOVERNING LAW AND JURISDICTION

10.1 Governed by laws of Singapore.

10.2 Jurisdiction: Singapore courts.

SCHEDULE 12

AUSTRALIA (PRIVACY ACT 1988)

1. DEFINITIONS

1.1 “Australia Privacy Act” means the Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs).

1.2 “APP Entity” means Customer.

1.3 “Processor” means Bigstrum Solutions Private Limited.

1.4 Terms shall have meanings under the Privacy Act.

1.5 All references interpreted under Australian law.

2. TRANSFERS OUTSIDE AUSTRALIA

2.1 Cross-border disclosure permitted only where:

Reasonable steps ensure compliance with APPs; or

Consent or exception applies

2.2 Bigstrum shall ensure equivalent safeguards.

3. CONTRACTUAL SAFEGUARDS

3.1 This DPA ensures:

Compliance with APPs

Data protection obligations

4. PROCESSING OBLIGATIONS

4.1 Bigstrum shall:

Process per instructions

Implement security controls

Assist compliance

5. DATA SUBJECT RIGHTS

Includes:

Access

Correction

dsar@bigstrum.in (mailto:dsar@bigstrum.in)

6. DATA BREACH

6.1 Notification under Notifiable Data Breaches (NDB) scheme.

7. SUB-PROCESSING

Allowed with safeguards.

8. DATA RETENTION AND DELETION

Limited retention.

9. RESTRICTIONS

No unauthorized use or disclosure.

10. GOVERNING LAW

Australia.

SCHEDULE 13

JAPAN (ACT ON THE PROTECTION OF PERSONAL INFORMATION – APPI)

1. DEFINITIONS

1.1 “APPI” means the Act on the Protection of Personal Information (Act No. 57 of 2003), as amended.

1.2 “Personal Information Handling Business Operator” means Customer.

1.3 “Processor” means Bigstrum Solutions Private Limited.

1.4 Terms defined per APPI.

1.5 All references interpreted under Japanese law.

2. INTERNATIONAL DATA TRANSFERS

2.1 Transfers allowed where:

Adequate protection ensured; or

Consent obtained; or

Equivalent safeguards implemented

2.2 Bigstrum shall ensure safeguards.

3. CONTRACTUAL SAFEGUARDS

3.1 Incorporates obligations ensuring APPI compliance.

4. PROCESSING OBLIGATIONS

4.1 Bigstrum shall:

Process per instructions

Ensure security

Maintain confidentiality

Assist compliance

5. DATA SUBJECT RIGHTS

Includes:

Access

Correction

Suspension of use

dsar@bigstrum.in (mailto:dsar@bigstrum.in)

6. PERSONAL DATA BREACH

6.1 Notification obligations aligned with PPC requirements.

7. SUB-PROCESSING

Allowed with safeguards.

8. DATA RETENTION AND DELETION

As required.

9. RESTRICTIONS

No unauthorized processing.

10. GOVERNING LAW

Japan.