User Access Agreement

Straive provides its employees access to the Company's Information Technology resources, including computers, networks and systems for the purpose of performing services on behalf of the company or for performing activities in connection with his/her employment.

This agreement is made by and between **Spi Technologies India Private Limited.,** (Company) and _____Parkavan_Suriyaprakasam___ (Employee).

During the course of employment with the Company:

1 The Employee shall comply at all times with the Company's Information Security policies and procedures of which the Employee has been made aware. The Employee who has committed a security breach shall be subjected to a formal disciplinary process as per Employee Code of Conduct;
2 The Employee shall not use the system to initiate unauthorized access to other systems nor use any information technology resources of the Company in order to obtain access to any network or system, or elsewhere, for which the person has not been authorized. Under no circumstance shall the Employee disclose any information that allows any third person access to the Company's system from a remote location;
3 The Employee shall have a unique user ID for accountability reasons. The Employee is responsible for all actions performed using their account. Only the immediate superior of the Employee can request a new user account or additional access privileges for the Employee. The Employee shall only be granted specific system access rights and privileges required to perform their assigned work tasks as approved by their immediate superior and assigned by Corporate IT;
4 The Employee shall define a secure password to access their account. The Employee shall not share or display this password in any manner. Likewise, The Employee shall not use any automatic login and/or password script routines / programs.
5 The Employee shall not leave their workstation unattended with any Internet, Email or major application open;
6 The Employee shall not use Company Email for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facility, or unwarranted or unsolicited interference with others' use of e-mail or email systems (such as sending or forwarding e-mail chain letters, exploiting email servers or resending the same e-mail repeatedly to one or
more recipients to interfere with the recipient's use of e-mail). The Employee must be aware of computer viruses and other destructive computer programs and take steps to avoid being their victim;
7 The Employee shall not install any software or hardware on their workstation at any time without the prior written permission from Corporate IT;
8 The Employee shall make every effort to protect the computer equipment assigned to them from hazards such as liquids, food, smoke, etc;
9 The Employee shall promptly report all information security incidents to their supervisor. 10 The Employee should oblige the Mobile Phone Usage Policy

This Agreement has been explained to the Employee in a language known to him/her. The Employee understands and agrees that any violation of this Agreement shall entitle the company to bring the appropriate legal action against him/her. In addition, any breach or violation of this Agreement may constitute a ground for termination of employment with the Company.

Conformer: Parkavan Suriyaprakasam

(Employee Signature over Printed Name)

Date: 10/03/2025

CONFIDENTIALITY
AND
NON DISCLOSURE AGREEMENT

This Confidentiality and Non-Disclosure Agreement ("**Agreement**") is made at

____Perambalur_____ (location) on this _____10/03/2025_____

[date, month, year]

BY AND BETWEEN

SPI TECHNOLOGIES INDIA PRIVATE LIMITED, a company under the provisions of Companies Act, 2013 having its Corporate Identification Number U93000PY2017PTC008168 having its registered Office at RS no: 4/5 & 4/6, Gothi Industrial Estate, Kurumbapet, Puducherry – 605 009, India (hereinafter referred to as "**Straive"** which expression shall, unless repugnant to the context thereof, be deemed to mean and include its legal representatives, successors-in

interest and permitted assigns) of the One Part

AND

_____Parkavan_/_412513_____ [Employee Name/Code] (hereinafter referred to as "Employee" which term shall mean and includes himself / herself, his (or) her legal representatives, successors-in–interest and assignees) of the Other Part

"Straive" and "Employee" shall hereinafter be individually referred to "Party" and collectively referred to herein as "Parties".

PREAMBLE

WHEREAS Straive is engaged in the business of data processing and related services, primarily in the typesetting business, including the transformation of unedited manuscripts, supply of structured data and providing end–to-end management services, various management/ and or consultancy services, corporate support services and corporate secretarial services (hereinafter referred to as "Business");

AND WHEREAS the Employee is employed with Straive for the monthly salary and rendering the services towards the Business of the company;

AND WHEREAS Straive intends to engage the services of the Employee to provide requisite services as warranted for its Business operations;

NOW, THEREFORE, in consideration of the mutual covenants and agreements contained herein, the Parties agree as follows:

1. Confidential Information

The term "Confidential Information" will mean any information whether in verbal (or) written form, may include, but is not limited to SPI's business, operations, infrastructure, business plans, software, marketing strategies, trade secrets, financial information including pricing, technical information including research, development, procedures, algorithms, data, drawings, designs including but not limited to trademark, service mark, logos, trade name, corporate name, any intellectual property or any guideline to use such designs, know-how, business information, including operations, products and their features, customer and their data including personal information and data, terms of any agreement between the Parties and discussions, negotiations and proposals related thereto including any comments, observations, remarks, inputs made in any meetings between the Parties, originally disclosed by Straive ("**Disclosing Party**") to the Employee ("**Receiving Party**") under this Agreement, in form, tangible, written,

electronic, in the form of samples, models, presentations (or) charts. The information will be considered as Confidential Information irrespective of whether it is marked as "confidential" or not while disclosing by Straive. If the Confidential Information is transmitted verbally, Straive shall within a reasonable period of time reduce the verbal communication into writing indicating that such verbal communication constituted Confidential Information and transmit the written communication to the Receiving Party. Notwithstanding this provision, if the Disclosing Party fails to reduce the verbal communication into writing, the obligation of the Receiving Party to treat the verbal communication as confidential under this Agreement shall remain in force.

2. Protection of Confidential Information

2.1. The Receiving Party understands and acknowledges that the Confidential Information has been developed or obtained by the Disclosing Party after investment of significant time, effort and expenses, and that while the Confidential Information may not be novel, unique, patentable, copyrightable, or constitute a trade secret, the Confidential Information disclosed to the Receiving Party is a valuable, special and unique asset of the Disclosing Party. Therefore, the Receiving Party agrees to hold in confidence and shall, at no time from the date of the agreement directly or indirectly disclose make known, divulge, publish or communicate the Confidential Information to any person, firm, or corporation, or use the information for its own benefit except for the purpose described hereinabove without the prior written consent of the Disclosing Party. The Receiving Party shall protect the Confidential Information and will use the same standard of care as it would use to secure and safeguard its own Confidential Information of similar nature and importance, but in no event shall it use less than reasonable care to prevent the unauthorized use and dissemination as the Receiving Party uses to protect its own confidential information.

2.2. The obligation of the Receiving Party to ensure and maintain Confidential Information of the Disclosing Party shall remain and valid for the period of three (3) years even if the agreement is terminated or cancelled between the Parties for whatsoever reason.

2.3. Employee shall duly comply with Straive Corporate Governance Policies, Conflict of Interest Policy, Global Data Privacy Policy and the International Data Privacy/Protection Legislations at all times during the entire course of employment with Straive.

2.4. The Receiving Party will use the Confidential Information only for the purpose of rendering Business services.

2.5. The Receiving Party will not copy or modify any Confidential Information without the prior written consent of the Disclosing Party. Any permitted reproduction of Confidential Information must contain all confidential or proprietary legends which appear on the original. The right to copy and modify the Confidential Information shall not inure any

intellectual property rights or ownership interest in the Confidential Information on the Receiving Party.

2.6. The Confidential Information and all proprietary rights associated therein shall remain the property of the Disclosing Party. The Receiving Party shall at all times comply with Straive confidential and/or proprietary information including source code and related documentation and further shall comply with SPi's Policies related to intellectual property rights, specifically pertains to ownership, permissible use and management of source code. Employee unequivocally confirms that Straive

exclusively owns all software code and related software documentation entrusted to Employee to enable him to render his/her services connected with the Business operations. The Employee shall not copy any source code to any personal machine or in any manner appropriate the same for personal use or unauthorized distribution to other parties without prior specific written consent issued by an authorized Officer of the company. Employee further agrees that any breach of this provision shall result in immediate imposition of disciplinary action and/or pursuit of appropriate legal reliefs before the competent forum at the cost and consequences of the Employee.

2.7. Confidential Information shall not be disclosed or transferred to any third party without the specific prior written approval of the Disclosing Party.

2.8. The protection of personal information applies to the Receiving Party and extends to SPi's clients personal information. Any personal information may it be personal or sensitive in nature that will be known, requested, processed, and used by the Receiving Party in any media forms (hard and electronic copies) to perform his (or) her services with the Disclosing Party shall not be disclosed to other parties without prior written consent from the Disclosing Party.

2.9. The Receiving Party shall (i) notify the Disclosing Party promptly of any material unauthorized possession, use or knowledge, of the Disclosing Party's Confidential Information by any person or entity which comes to knowledge of the Receiving Party ; (ii) promptly furnish to the Disclosing Party to the best of its knowledge full details of the unauthorized possession or use ; (iii) reasonably assist the Disclosing Party in investigating

or preventing the recurrence of any unauthorized possession, use of Confidential Information at the cost of Disclosing Party; and (iv) use reasonable efforts to cooperate with the Disclosing Party in any litigation and investigation against third parties deemed necessary by the Disclosing Party to protect its proprietary rights at the cost of Disclosing Party.

2.10. If it appears that the Receiving Party has disclosed or disseminated (or has threatened to disclose or disseminate) Confidential Information in violation of this Agreement, the Disclosing Party shall be entitled to seek all legal remedies including remedy in equity, injunction to restrain the Receiving Party from disclosing or disseminating, in whole or in part, the Confidential Information. Such injunctive relief shall be in addition to any other remedies available to the Disclosing Party, whether at law or in equity. The Disclosing Party shall be entitled to recover its costs and fees, including reasonable attorney's fees, incurred in obtaining any such relief. The Disclosing Party shall not be prohibited by this provision from pursuing other remedies, including a claim for losses and damages.

3. Exceptions

3.1. The following shall not be deemed Confidential Information. However, the onus of proving these exceptions lies solely with the Receiving Party.

i) Any information that is in public domain or that enters the public domain after that other than through the fault of the Receiving Party; or

ii) Any information required to be disclosed by the Receiving Party pursuant to order, directions of court of law or government authority; provided that the Receiving Party uses reasonable efforts to give the Disclosing Party reasonable advance notice of such required disclosure, to the extent practical and legally permissible upon receipt of notice directing the disclosure of Confidential Information.

4. Return of Confidential Information

Upon request of the Disclosing Party, the Receiving Party shall return to the Disclosing Party all written including electronic copies containing the Confidential Information. Similarly, on such request, the Receiving Party will destroy the Confidential Information of Disclosing Party contained in electronic form. The Receiving Party shall also confirm in writing that it has returned and destroyed all the tangible and electronic Confidential Information within seven (7) days of receipt of the aforesaid written request.

5. Relationship of Parties

This Agreement is intended to facilitate only the exchange of Confidential Information and consequent protection of Confidential Information and is not intended to be, and shall not be construed to create any joint venture (or) partnership.

6. No Grant of Property Rights

The Receiving Party recognizes and agrees that, except as expressly and specifically set forth in this Agreement, nothing herein shall be construed as granting any right, by license, implication, estoppel or otherwise, to any of the Disclosing Party's Confidential Information, or to any invention or any patent right that was issued or that may be issued based on such Confidential Information. All information disclosed is provided "as is" without any warranties of any kind.

7. General Provisions

7.1. This Agreement sets forth the entire understanding of the Parties regarding confidentiality.

7.2. Any known relationship and/or affiliation with any stockholder, director, officer, employee, supplier, contractor, consultant, agent of the Disclosing Party should be immediately disclosed by the Receiving Party to the vendor accreditation management of the Disclosing Party.

7.3. The Receiving Party obligates himself (or) herself to take further steps, actions or measures in order to comply with other requirements as may be given by the Disclosing Party such as, but not limited to, periodic disclosure of relationships and/or affiliations with any of the Disclosing Party's stockholder, director, officer, employee, supplier, contractor, consultant, agent or their relatives.

7.4. This Agreement shall not be assignable by either Party, and neither Party may delegate its obligations under this Agreement, without prior written consent of the other Party.

7.5. This Agreement shall not be amended, modified, released, discharged, abandoned or otherwise terminated prior to expiration, in whole or in part, except by written agreement signed by the parties hereto.

7.6. In the event that any provisions or any portion thereof, of this Agreement is declared to be invalid, unenforceable or prohibited by applicable law, such provision or part thereof shall be inoperative only to the extent of such prohibition, without affecting validity of remaining provisions of the Agreement.

8. Disputes

In the event of any disputes and differences between the Parties arising out of or in connection with this Agreement shall be referred to a Sole Arbitrator to be appointed by the Disclosing Party, in accordance with the provision of the Arbitration and Conciliation Act, 1996 (or) any of its amendments thereto. The place and seat of Arbitration shall be at Chennai, India and the language shall be English. The decision of the arbitrator shall bind the Parties. Cost of the arbitration proceedings in its entirety shall be borne by the respective Party as decided in the arbitral award.

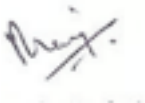
9. Governing Law and Jurisdiction

This Agreement shall be construed under the laws of India. All disputes arising out of or in connection with this Agreement shall be subject to the exclusive jurisdiction of the appropriate courts in Chennai, India only.

10. This Agreement will commence on the date first set forth above and will remain in effect for two (2) years from the date of last disclosure of Confidential Information by either party, at which time it will terminate.

IN WITNESS WHEREOF THE PARTIES HAVE SET THEIR HANDS AND SUBSCRIBED THEIR RESPECTIVE SIGNATURE ON THIS THE DAY, THE MONTH AND THE YEAR HEREINABOVE WRITTEN AND IN THE MANNER HEREINAFTER MENTIONED.

for **Spi Technologies India Pvt. Ltd.,**



Authorised Signatory

Employee Name Signature with Date Employee Code : Parkavan Suriyaprakasam,

10/03/2025 - 412513

In the Presence of:

1 2

Signature		
Name/Emp. Code		
S/o or **D/o** or **W/o**		
Residential Address		

HR/IN-20/0008 rev. 01

DATA PROTECTION NOTICE
FOR STRAIVE PERSONNEL AND NON-EMPLOYEE RESOURCES

Introduction

In compliance with the applicable laws, standards and regulations governing the processing of personal information, as may be amended or enacted from time to time, including, but not limited to: the EU General Data Protection Regulation 2016/679 ("GDPR"); any national laws which implement the GDPR; the UK Data Protection Act 2018; the U.S. Health Insurance Portability and Accountability Act ("HIPAA"); the U.S. Gramm-Leach-Bliley Act ("GLBA"); the California Consumer Privacy Act of 2018 ("CCPA"); the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"); the Australian Federal Privacy Act 1988 and Privacy Amendment (Enhancing Privacy Protection) Act 2012; the Swiss Federal Act on Data Protection ("DPA"); India's Information Technology Act 2000; Japan's Act on Protection of Personal Information ("APPI"); the Payment Card Industry Data Security Standard ("PCI DSS"); Republic Act 10173 or otherwise known as Data Protection Act of 2012 ("**DPA**"); any fair information practices for handling, storing or managing data with privacy, security, and fairness that are incorporated into the foregoing or any other applicable laws or regulations and, where applicable, any guidance and codes of practice issued by any standards authority or government regulator or authority established in a particular jurisdiction which govern the processing of Personal Information, Straive Group of Companies,(collectively, "**Straive**") seeks your consent to collect and use your personal data for the purposes defined in this Notice ("**Purposes**").

Collection and Processing of Personal Data

Straive maintains certain personal information about you as part of our general personnel records, inclusive of direct employees and non-employee resources. Our records may include, among others, your full name, employee number, position title, contact numbers, mailing and email addresses, Government ID numbers (Aadhaar Card/Pan Card/Driving Licence/ Ration Card/ any other agreeable Govt documents), marital status, educational background, employment application, history with the company, areas of expertise, details of salary and benefits, bank details, performance appraisals and salary reviews, records relating to holiday and other leave, working time records and other management records.

Straive obtained this information directly from you without any coercion, undue influence beginning with your application for a role within the company either as a direct employee or non-employed resource and throughout such entire employment/contract life cycle leading up to or including your exit from

Straive. Straive will receive and/or retain the information in various forms (whether in writing, electronically, verbally or otherwise). Straive have also obtained some of these information, by your express consent and/or by force of our legal and contractual relations, from public offices, private enterprises and individuals and you voluntarily agree without any demur (or) protest.

Straive uses this information for a variety of personnel/resource administration, work and general business management purposes, information to administer payroll, improve and maintain the administration of employee benefits (leave entitlement, insurance, other applicable benefits), facilitate the management of work and employees, operate performance and salary reviews, operate the Company's IT security and communications systems, comply with record keeping and strict adherence of other legal obligations. The information will also be used in filling of government reports, handling of pre-employment, annual health check-ups, checking of background (for hiring purposes), analysis of Manpower (organization diagnosis and total rewards review), management reporting, corporate events and other incidental activities thereto.

Straive also processes information relating to your health which may amount to sensitive personal data. The particular information that the company holds relating to your health is the records of sickness absence and medical certificates/medical reports which have been provided (or) directed to be submitted.

Security of your Personal Data

The information is placed in duly protected databases and controlled by the local HR Team. Some of this personal information is stored in a database located at the respective offices of Straive. Straive has security measures in place which ensures the confidentiality of the information contained in the database and these measures will be reviewed over time and upgraded in line with technological developments. The remainder of the personal information is held on personnel files which are kept in the designated places at the respective locations, which is duly maintained by the respective location HR Team.

Retention, Management and Deletion of your Personal Data

Your personal data in digital and/or physical forms will be retained, managed, or deleted in accordance with the guidelines and controls set in the Straive Data Governance Policy, Human Resources Security Policy, Confidentiality and Data Privacy Policy, Document and Records Control Procedure of Straive and all applicable laws.

Disclosure to Third Parties

Straive will not disclose your personal data to any third party without your consent except: 1. to our parent

(or) holding company, subsidiaries, affiliates, group companies, related and associated companies;

2. to our business partners, affiliates, clients and third party service providers; 3. to the extent permitted by law, to any third party credit agency including but not limited to banking institution for payroll processing

4. to any financial institution in connection with your loan/ financing application required or requested by you, or in connection with background verification;

5. to our business partners (clients) who require Personal Identifiable Information (PII) as part of their information security policy before enrollment, modification, and/or creation of user access to their VPN, various systems and/or applications to fulfill the job or task required.

6. lawfully permitted or required under the law or in relation to any order, direction, decree or judgment of a court

7. required for the purpose of prevention of crime, illegal/unlawful activities or fraud or for the apprehension or prosecution of offenders or for an investigation relating to any of these; 8. required to protect our rights and defend the interest of Straive, its assets and property; 9. required or requested by you; and

10. required to carry out any of the Purposes stated above

Employee's Consent

I confirm that I have read and understood this **DATA PROTECTION NOTICE** and hereby consent to the collection and processing of my Personal Data and Sensitive Personal Data as defined in the applicable laws and all other applicable data privacy regulations in accordance with the requirements under the Notice for all purposes relating to my employment with Straive as explained in this notice. Further to the above, I hereby agree to comply with all reasonable request of Straive to enable the organization's compliance with its obligations under the applicable laws, regulations and/or guidelines.

_____Parkavan Suriyaprakasam / 10/03/2025_____

Signature over printed name / Date

In the Presence Of :-

1)

2)