PARTNERS IN PROSPERITY
Enriching people, and planet

SOP Document Tracker

1	SOP No.	S0009	
2	Doc. ID*	S0009Admin18022018	
3	Title	**Data Protection Policy**	
4	E-file name	E:\Pnp Documents\Sops Of Pnp\Policies\Sop 9 Data Protection Policy.Docx	
5	Date of Expiry	Until notified	
6	Dates Previous 2 Versions		
7	Date of withdrawal		
8	Holder Name and Designation	Manager – Administration for Admin related documents	
9	Authorized Issuer	Mr. Manab Chakraborty, CEO	
10	Signature of the issuer		
11	Date of Signature	1/04/2019	

PS: *This document replaces all previous versions, if any.

Data Protection Policy

1. Purpose and Scope

1.1 The purpose of Data Protection Policy (this Policy) is to set out the process and the framework within which to collect, use and protect Personal and Sensitive Data, and this Policy shall apply to all Individuals working for PNP / Individual Employees (as defined in Section 1.3, below). The Policy states how PNP collects, uses, processes and safeguards the Personal Data and Sensitive Personal Data that it possesses, holds, and deals with, in accordance with the applicable Data Protection Law.

1.2 This Policy should be read in conjunction with PNP's other policies, including the Human Resource (HR), Whistle Blower Protection policy and Finance Policies.

1.3 This Policy applies to all employees, consultants, managers, officers, directors, employees (whether permanent, fixed term or temporary), consultants, contractors, volunteers, interns, home workers, part-time workers and agency workers of PNP,and their permitted affiliates, successors, group companies, affiliates, subsidiaries and assigns (together known as "PNP").

2. Policy Key terms

The key terms used in this Policy are defined in Annexure A.

3. Data Protection Obligations

3.1 As required by Data Protection Law, the following rules or "Principles" shall apply:

- **Principle 1:** Personal Data shall be processed fairly and lawfully;
- **Principle 2**: Personal Data shall be obtained only for specified and lawful purposes, and must not be processed in a manner which is incompatible with those purposes;
- **Principle 3:** Personal Data must be adequate, relevant and not excessive in relation to the purposes for which it is processed;
- **Principle 4:** Providers of Personal Data must, as and when requested, review the Personal Data and ensure that the Personal Data is accurate and, where necessary, kept up to date;
- **Principle 5:** Personal Data processed for any purpose shall not be kept for longer than is necessary or is otherwise required under any other law for the time being in force;
- **Principle 6:** Appropriate measures shall be taken against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, or theft of Personal Data; and
- **Principle 7:** Personal Data shall not be transferred to a country outside India unless the transferee entity ensures the same level of data protection that is adhered to by PNP. Personal Data shall be transferred only if it is necessary for the performance of a lawful contract between PNP and the transferee entity, subject to prior permission from the provider of Personal Data.

3.2 **Collection, Use and Processing of Personal Data:** PNP would use Individual's Personal Data for lawful purpose and only in connection with employment or the provision of goods, services to PNP, and it will ensure that such use is "fair" and "lawful". PNP would use Personal Data after seeking Individual's consent in accordance with the Consent Letter provided in Annexure E, and in ways that the Individual would reasonably expect, and not in a manner that would have unjustified adverse effects on him or her. PNP will endeavour to be compliant with the relevant laws of India while giving effect to the Policy. Further details on collection, use and processing of personal data are provided in Annexure B to this Policy. However, PNP may process the Personal Data of any person without the consent of the person concerned for any of the following purposes:

(a) the prevention or detection of crime;

(b) the prosecution of offenders; and

(c) the assessment or collection of any tax or duty.

3.3 **Security:** PNP shall adopt Reasonable Security Practices and Procedures, in accordance with Rule 8 of the IT Rules, 2011, to protect Personal Data from accidental loss, theft, destruction, damage, unauthorised or unlawful processing. In addition to the PNP's obligations in this respect, it is incumbent upon Individual Employee and any other person to whom this Policy may apply, to comply with and take the steps contained in Clause 1- 4 of Annexure C to this Policy.

4. **Use of Individual's Personal Data by PNP** - This Section of the Policy explains how PNP intends to uses an Individual's Personal Data. Refer Annexure D of this Policy.

5. **Data Transfer to Third Party**

PNP may authorise a third party to access and process Individuals Personal Data subject to putting in a procedure that is compliant with Data Protection Law.

Where PNP or any of its affiliated entity hires a third party, such third parties may include:

a. other members of the PNP group, including their employees, directors and officers;

b. PNP's or other members of the PNP group's clients or customers;

c. service providers, business associates, professional advisors, auditors and suppliers;

d. local or foreign regulators, governments, law enforcement authorities (including tax, social or labour authorities), courts, tribunals, arbitrators or other judicial committees;

e. any person in connection with any sale, merger, acquisition, disposal, reorganisation or similar change of PNP's (or any other member of the PNP

group's) business or assets (including any potential or actual purchaser of the business or assets and their advisors);

f. financial organisations; g. education and training organisations; and

h. employment and recruitment agencies, and your past or prospective employers.

6. **PNPindividual rights and access to information**

   PNPwill maintain accurate and up to date Personal Data about each Individual as provided by the Individual. All Individuals shall have access to their own Personal Data. Individuals must regularly review and update their Personal Data that PNP holds in order to ensure that the Personal Data is correct and accurate. An Individual may request PNP to cease use of their Personal Data, and in such situation the Individual may contact the Data Protection Officer. Individual will have a right to request a copy of your Personal Data held by PNP. If the Individual would like to exercise any of their rights or require further information about how PNPuses the Individual's Personal Data, then such information may be sought from the Administrative Manager.

7. The Data Protection Officer

PNP, Data Protection Officer is Sreelatha R. (AdministrativeManager).

The Data Protection Officer's contact details are as follows:

Email: info@pnpindia.org.in

Telephone: +91 9971594778

The Data Protection Officer shall ensure implementation of this Policy, and shall make the Policy available to Individuals and redress the grievances of the provider of Personal Data expeditiously within one month from the date of receipt of grievance. The Data Protection Officer in consultation with PNP management will update the Policy as required from time to time. In the absence of the Data Protection Officer please contact your supervisor.

8. **Compliance of the Policy**

   Compliance with this Policy is essential to ensure that appropriate controls are in place. Any Individual Employee or Individuals Working for PNP (defined in Para 1.3) found to have intentionally violated this Policy may be subject to suitable action including disciplinary action, up to and including termination of employment/ contract under the applicable law.

Annexure A- The Key Terms

- **"Consent Letter"** means the format of letter provided in Annexure E hereto, to be procured from the provider of Personal Data in writing or by any mode of electronic communication.

- **"Data Protection Law"** means the laws governing the protection of Personal Data that PNP is obliged to comply with, including the Information Technology Act, 2000 ("IT Act") read with Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, of India, as amended from time to time. These laws impose obligations on those, who collect, possess and process Personal Data (such as PNP) and grant rights to Individuals or persons against misuse of such data

- **"Data Protection Officer"** meansPNP's designated 'data protection officer'.

- **"Personal Data"**shall mean, any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

- "**Process",** "processing" Data Process/ Processing has not been defined under the Act. However, an "intermediary" has been defined under clause (w) of sub-section (1) of section 2 of the Information Technology Act, 2000 with respect to any particular electronic message as any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.

- "**Sensitive Personal Data"** Sensitive personal data or information of a person under the Data Protection Law, means such personal information which consists of information relating to;— (i) password;(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;(iii) physical, physiological and mental health condition;(iv) sexual orientation;(v) medical records and history;(vi) Biometric information;(vii) any detail relating to the above clauses as provided to body corporate for providing service; and(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

- **"Rule 8 of the IT Rules 2011" Reasonable Security Practices and Procedures.**
  1) A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information

security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.

2. The international Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub-rule (1).

3. Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule (1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.

4. The body corporate or a person on its behalf who have implemented either IS/ISO/IEC27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried cut by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource.

Annexure B- Collection, Use and Processing of Personal Data

1. PNPmust have lawful purpose for processing Personal Data. Generally, this will require the following conditions to be met:
   I. the Individual has clearly consented to the collection and processing of his/her Personal Data in terms of the consent letter annexed hereto;
   II. the collection and processing are necessary: (a) to perform a contract with the Individual; or (b) to take steps at the request of the Individual in order to enter into a contract;
   III. the collection and processing are necessary to comply with a legal obligation (but not a contractual obligation) to which PNPis subject.

2. The processing is necessary for the purpose of PNP's legitimate business interests and does not unduly prejudice or harm the interests of the Individual. PNP shall ensure that certain information standards are applied to the Personal Data processed by PNP:
   I. Only collect and use such Personal Data as is necessary for the purpose for which it is collected and not collect Personal Data more than is required for that purpose;

   II. Ensure that Personal Data is updated in the company records, as provided by the Individual.

   III. Ensure that PNP does not hold the Personal Data for longer than is necessary, taking into account its purpose; any legal or regulatory obligations to retain the Personal Data.

   IV. Ensure that Individual's understand how PNP uses their Personal Data, in particular, when an Individual provides their Personal Data, that Individual should be told (prior to his or her Personal Data being processed):
   - who will be processing the Personal Data (e.g. PNPor another entity within the PNPgroup);
   - the purposes for which the Personal Data are being collected and processed; and
   - Any other information that is necessary to enable the processing of the Individual's Personal Data to be fair.

   V. Sensitive Personal Data shall be collected and processed only after seeking the Individual's consent in terms of the Consent Letter annexed hereto.

   4. Please contact the Data Protection Officer to obtain the standard document to collect Personal Data and for more information. Any decision not to provide this information must be referred to the Data Protection Officer.

Annexure C- Security Measures to protect Personal Data

1. Adherence to PNPAccounts, HR and Whistle Blower Policies, as well as any specific guidelines issued by PNP from time to time;
2. Installation of appropriate measures to prevent data being accessed or used by any unauthorised person;
3. Not disclose Personal Data to, or make alterations to Personal Data at the request of, a third party (including law enforcement or regulatory bodies) unless the Individual is sure that the third party has been authorised by PNP to receive such information or make such requests; if you are in doubt, you must contact the Data Protection Officer before disclosing the Personal Data; and
4. Contact the Data Protection Officer immediately if any Individual suspects that the security of any Personal Data has been compromised (e.g. if Personal Data has been lost, stolen or accessed by any unauthorised person).
5. Where PNP intends to engage a service provider, third party or other member of the PNPgroup to process Personal Data on PNP's behalf, it would consult the Data Protection Officer for ensuring security of the data, prior to disclosing any Personal Data to the service provider, third party or other member of the PNP group.

Annexure D- Use of Individual's Personal Data

PNP may itself or through a third party, service provider or a member within the PNPGroup, process your Personal Data, including Sensitive Personal Data and disclose your Personal Data to third parties, for a variety of business purposes including, without limitation, the following:

a. performing our obligations in connection with your employment with (or engagement by PNPincluding in relation to recruitment, the provision and checking of references, personnel performance management, review and professional development, payroll, fund management and accounting (including for the payment and review of salaries and other benefits), pensions administration, and insurance administration;
b. managing and operating PNP's or other members of the PNPgroup's businesses, technology infrastructure, support and facilities (including in relation to the operation and monitoring of our systems and facilities) and managing PNP's or other members of the PNPgroup's property;
c. advertising, marketing and developing the business of PNPor other members of the PNP group and promoting public relations in relation to the same;
d. administering relationships with customers and suppliers;
e. preventing and detecting breaches of law, and apprehending and prosecuting offenders (including through the use of CCTV);
f. complying with law, regulation, guidance or rules, demands or requests made by local and foreign regulators, governments and law enforcement authorities, including tax collection agencies and stock exchanges (whether or not having the force of law) or any court order or court process, or in connection with any litigation (including any discovery or disclosure process in connection with litigation);
g. in connection with any sale, merger, acquisition, disposal, reorganisation or similar change of PNP's or another member of the PNP group's business or assets, including any due diligence or similar process carried out in connection with such a transaction; and
h. Any other purpose that is incidental to or connected with the foregoing purposes or otherwise in the course of PNP's legitimate business.
i. Where it is necessary and reasonable for PNP to do so, it may continue to process Individual Employee's Personal Data following the cessation of his or her employment with (or engagement by) PNP.

ANNEXURE E – Consent Letter

To,
Administrative Manager
Partners in Prosperity
1 B/1 Taj Apartments, Rao Tula Ram Marg,
New Delhi 110022

Dear Sir/Madam,

I, _____, hereby authorisePartners in Prosperity, 1 B/1 Taj Apartments, Rao Tula Ram Marg, New Delhi 110022, to collect and process my Personal Data provided by me to PNPfor the purposes necessary for its business and as stated in the Data Protection Policy. I have read and understood the Data Protection Policy and I also agree to update any change/modification to the personal data provided by me to PNP.

I understand that the Personal Data provided may be transferred to, and stored at, countries outside of India and the Personal Data may be shared with other international associate companies of PNPor member of the PNP Group, I hereby consent to transfer of my Personal Data to a third party if necessary, for the business of PNPor for the performance of any lawful contract betweenPNP and any third party.

Name _____

Place: _____

Date: _____