Data Privacy Policy

Purpose

This Policy lays emphasis on the obligations of the Relevant Individuals dealing with the Data in the course of performance of their duties at SolCen Technologies Private Limited.

I. Definitions:

a. **Applicable Law** means the Information Technology Act, 2000 ("IT Act") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("IT Rules");

b. **Data** means collective reference to the Personal Data (defined thereafter) and Sensitive Personal Data (as defined thereafter).

c. **Personal Data** means 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, can identify such person. Processing refers to any action performed on Personal Data, such as collecting, recording, organizing, storing, transferring, modifying, using, disclosing, uploading or deleting.

d. **Sensitive Personal Data** means such Personal Data which consists of information relating to:

- Password;
- Financial Information such as bank account or credit card or debit card or other payment instrument details;
- Physical, physiological and mental health condition;
- Sexual orientation;
- Medical records and history;
- Biometric Information;
- Any other details relating to the above mentioned, provided by any person to SolCen for providing services;
- Any Information received pursuant to the above mentioned by SolCen for processing, or storing such Information under a 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 will not be considered to be Sensitive Personal Data.

e. **"Employee"** means a SolCen current or former employee. As far as it applies to Employees, the Policy covers all stages of the employment cycle including recruitment and selection, promotion, evaluation and training.

f. **"Relevant Individual"** means an Employee, contractor and/or any other third party working on SolCen's behalf and job applicants who have signed the employment agreement with SolCen.

g. **SolCen** shall mean SolCen Technologies Private Limited.

II. Applicability

a. This Policy is applicable to all the Data collected, received, possessed, owned, controlled, stored, dealt with or handled by SolCen in respect of a Relevant Individual, who upon their joining with the SolCen have signed the employment agreement and have gone through this Policy (as provided as part of the employment agreement) and have gone through the contents of this Policy and have given their explicit consent in writing to be bound by this Policy.

b. Data and information that SolCen handles for its clients in the context of providing consulting, technology and outsourcing services shall be processed according to the contractual provisions, specific privacy practices agreed upon with each client, as applicable.

III. Scope of Coverage

a) Collection of the Data by SolCen

Throughout the course of the relationship with the Relevant Individual, SolCen needs to collect the Data. The type of Information that may be collected includes (but" is not limited to), where relevant:

- Basic Information regarding the Relevant Individuals such as name, contact details, address, gender, birth date, marital status, children, parents details, dependent details, photos, photo id proof, pan card, passport, voter ID, Aadhar card, life

insurance nominees/beneficiaries, fingerprint information, emergency contact details, citizenship, visa, work permit details;

- Recruitment, engagement or training records including curriculum vitae, applications, notes of interview, applicant references, qualifications, education records, test results (as applicable);
- Information about the Relevant Individual's medical condition – health and sickness records;
- The terms and conditions of employment/engagement, employment contracts with SolCen and/or previous employer;
- Performance, conduct and disciplinary records within SolCen and/or with previous employers; mobility records generated in the course of employment/work with SolCen;
- Information relating to the Relevant Individual's membership with professional associations or trade unions;
- Leave records (including annual leave, sick leave and maternity leave);
- Financial Information relating to compensation, bonus, pension and benefits, salary, travel expenses, stock options, stock purchase plans, tax rates, taxation, bank account, provident fund account details;
- Information captured as result of monitoring of SolCen assets, equipment, network owned and/ or provided by SolCen;
- Any other Information as required by SolCen.

b) Purposes of collection and processing of the Data

SolCen may collect, process and disclose the Data of the Relevant Individual for purposes connected with its business activities including the following purposes, hereinafter the "Agreed Purposes":

- Managing the Relevant Individual's employment/ work with SolCen including deployment/assignment of the individual to specific client projects;
- Record-keeping purposes; payroll administration, payment of the Relevant Individual's salary or invoice;
- Performance assessment and training purposes;
- Compliance with the legal requirement(s)/obligation(s);
- health and safety rules and other legal obligations;

- Administration of benefits, including insurance, provident fund, pension plans; immigration, visa related purposes;
- Background verification purposes; credit and security checks;
- Operational issues such as promotions, disciplinary activities, grievance procedure handling;
- Audits, investigations, analysis and statistics, for example of various recruitment and employee retention programs;
- IT, security, cyber security and access controls;
- Disaster recovery plan, crisis management, internal and external communications;
- For any other purposes as SolCen may deem necessary.

SolCen only collects, uses and discloses the Data for purposes that are reasonable and legitimate. Such Data shall be processed in a manner compatible with the Agreed Purposes; unless the Relevant Individuals have consented to it being processed for a different purpose or the use for a different purpose is permitted by applicable law.

c) Limited Access to the Data

Only those Employees who "need-to-know" or require access to function in their role should have access to the Data. SolCen will not disclose the Data and/or the Sensitive Data to any person outside SolCen except for the Agreed Purposes, or with the Relevant Individuals' consent, or with a legitimate interest or legal reason for doing so, such as where SolCen reasonably considers it necessary to do so and where it is permitted by applicable law. In each instance, the disclosed the Data will be strictly limited to what is necessary and reasonable to carry out the Agreed Purposes. When SolCen works with third parties which may have access to the Data in the course of providing their services, SolCen contractually requires third party to process the Data only on SolCen's instructions and consistent with SolCen's Data Privacy policies and Data Protection laws.

d) Disclosure and Transfer of the Data

SolCen may, from time to time, disclose and/or transfer the Relevant Individuals' Data, to which such Relevant Individuals' have given their explicit consent while signing the employment agreement, to third parties (including but not limited) listed below:

- Group Companies, if any, affiliate companies and/or other business associates, SolCen's insurers and banks;
- External and internal auditors;
- Medical practitioners appointed by SolCen;
- Administrator of SolCen's mandatory provident fund scheme;
- Third parties who are involved in a merger, acquisition or due diligence exercise associated with SolCen;
- External companies or third-party service providers SolCen engages to perform Services on the SolCen's behalf;
- Third Parties providing certain information technology and data processing services to enable business operations;
- The applicable regulators, governmental bodies, tax authorities or other industry recognized bodies as required by any applicable law or guidelines of any applicable jurisdiction; and
- To any other party as deemed necessary by SolCen. Notwithstanding anything contained elsewhere, any Personal or Sensitive Personal Data may be disclosed by SolCen to any third party as required by a Court of Law or any other regulatory or any other law enforcement agency established under a statute, as per the prevailing law without the Relevant Individual's consent. instructions from SolCen and to take appropriate technical and organizational measures to ensure that there is no unauthorized or unlawful processing or accidental loss or destruction of or damage to the Data.

e) Retention and Deletion of the Data

It is SolCen's policy to retain certain Data of the Relevant Individuals when they cease to be employed/ engaged by SolCen.

This Data may be required for SolCen's legal and business purposes, including any residual activities relating to the employment/engagement, including for example, provision of references, processing of applications for re-employment/re-engagement, matters relating

to retirement benefits (if applicable) and allowing SolCen to fulfil any of its contractual or statutory obligations.

All Data of the Relevant Individuals may be retained for periods as prescribed under law or as per SolCen policy from the date the Relevant Individuals cease to be employed/engaged by SolCen.

The Data may be retained for a longer period if there is a subsisting reason that obliges SolCen to do so, or the Data is necessary for SolCen to fulfil contractual or legal obligations. Once SolCen no longer requires the Data, it is destroyed appropriately and securely or anonymized in accordance with the law.

f) Security of the Data

SolCen takes reasonable security measures to protect the Data against loss, misuse, unauthorized or accidental access, disclosure, alteration and destruction. SolCen has implemented policies and maintains appropriate technical, physical, and organizational measures and follows industry practices and standards in adopting procedures and implementing systems designed for securing and protecting the Data from unauthorized access, improper use, disclosure and alteration. SolCen cannot however ensure or warrant the security of any information the Relevant Individual transmits to the SolCen or guarantee that Relevant Individual's Personal Data and/or Sensitive Personal Data and/or other Non-Personal Information (as defined hereafter) provided for availing the Services or platform may not be accessed, disclosed, altered or destroyed by a breach of any of SolCen's security measures and safeguards. It is further clarified that Relevant Individual have and so long as such Relevant Individual accesses and/or uses the platform (directly or indirectly) the obligation to ensure that Relevant Individual shall at all times, take adequate physical, managerial, and technical safeguards, at such Relevant Individual's end, to preserve the integrity and security of its data which shall include and not be limited to Relevant Individual's Personal Data and/or the Sensitive Personal Data.

g) **Non – Personal and Automatic Information:** SolCen may also collect certain non-personal information, such as Relevant Individual's internet protocol address, web request, operating system, browser type, URL, internet service provider, IP address, aggregate user data, browser type, software and hardware attributes, list of third-party applications being used by the Relevant Individual, pages such Relevant Individual requests, and cookie information, etc. which will not identify with the Relevant Individual

specifically ("Non - Personal Information"), while such Relevant Individual browse, access or use the platform. SolCen receives and store Non – Personal Information, using data collection devices such as "cookies" on certain pages of the platform, in order to help and analyze the SolCen's web - page flow, track user trends, measure promotional effectiveness, and promote trust and safety. SolCen offers certain additional features on the platform that are only available through the use of a "cookie". SolCen places both permanent and temporary cookies in the Relevant Individual's computer's hard drive.

IV. Grievance Officer

Any questions, discrepancies, and grievances of the Relevant Individuals with respect to processing of the Data may be made to the SolCen Data Protection Officer (Grievance Officer) at kannan.s@solcen.in.

Notwithstanding the above, SolCen reserves the right to decline to process any such request which may jeopardize the security and confidentiality of the Data of others, as well as requests which are impractical or not made in good faith, or the circumstances as provided for under the law permitting SolCen to refuse such request(s).

V. Changes to Our Privacy Policy

SolCen reserves the unconditional right to change, modify, add, or remove portions of this Privacy Policy at any time, without specifically notifying the Relevant Individuals of such changes. Any changes or updates will be effective immediately. The Relevant Individuals should review this Policy regularly for changes. The Relevant Individuals may withdraw its consent if such amended Policy is not acceptable to it in manner as provided under this Policy.

VI. Employee Obligations

The Employee/Relevant Individual shall be diligent and extend caution while dealing with the Data of others, in the course of performance of his/her duties and shall also, at all times:

a. Prevent any un-authorized person from having access to any computer systems processing the Data, and especially:
b. un-authorized reading, copying, alteration, deletion or removal of data; un-authorized data input, disclosure, uploading, transmission/transfer of the Data;

c. Abide by SolCen's internal logistical and physical security policies and procedures;
   Ensure that authorized users of a data-processing system can access only the Data to which their access right refers;
d. Keep a record of which Data have been communicated, when and to whom; Not provide any Data to any third party without first consulting with his/her Manager or the Human Resources Department;
e. Ensure that the Data processed on behalf of a third party (client) can be processed only in the manner prescribed by such third party;
f. Ensure that, during communication of the Data and transfer of storage media, the data cannot be read, copied or erased without authorization;
g. Immediately, on becoming aware report and notify any vulnerabilities and privacy related breach/security breaches (including potential risks);
h. Attend mandatory and voluntary trainings on security and data privacy including e-learnings and online sessions.