POLICY

Data Privacy Policy

Dept. – Information Technology

Document-ID: **PL-C-IT-29**

Rev No. – 00, Rev. Date – 28.06.2022

1. Purpose

The purpose of this policy is to maintain the privacy of and protect the personal information of employees, contractors, vendors, interns, associates, customers and business partners of Plasser India Pvt Ltd and ensure compliance with laws and regulations applicable (refer annexure A ‘Data Privacy Annexures’ document) to Plasser India Pvt Ltd (hereafter referred to as “PI” or “the organization”).

2. Scope

This policy is applicable to all PI employees, contractors, vendors, interns, associates, customers, and business partners who may receive personal information, have access to personal information collected or processed, or who provide information to the organization.

This Policy applies to all PI employees, contractors, vendors, interns, associates, customers, and business partners who receive personal information from PI, who have access to personal information collected or processed by PI, or who provide information to PI, regardless of geographic location. All employees of PI are expected to support the privacy policy and principles when they collect and / or handle personal information or are involved in the process of maintaining or disposing of personal information. This policy provides the information to successfully meet the organization’s commitment towards data privacy.

All partner firms and any Third Party working with or for PI, and who have or may have access to personal information, will be expected to have read, understand and comply with this policy. No Third Party may access personal information held by the organization without having first entered into a **confidentiality agreement**.

3. Responsibilities

Person(s) responsible	HOD-IT

4. Terms / Definitions and abbreviations *(in alphabetical order)*

Dept.	Department
F	Format
FB	Faridabad
HOD	Head of Department
IT	Information Technology
KJ	Karjan
MD	Managing Director
MGMT	Top Management
PL	Policy
PR	Procedure
PI	Plasser India
Ref.	Reference
WI	Work instruction

5. Equipment/ Tools and environmental conditions

Equipment/ Tools	NA
Environmental conditions	NA

6. Environment, Occupational Health & Safety measures

NA	NA

7. Policy

Responsibilities

The owner for the Data Privacy Policy shall be the Head-IT or as nominated by MD (Refer Annexure 2 'Data Privacy Annexures' document). The Head-IT shall be responsible for maintenance and accuracy of this policy. Any queries regarding the implementation of this Policy shall be directed to the Head-IT.

This policy shall be reviewed for updates by Head-IT on an annual basis. Additionally, the data privacy policy shall be updated in-line with any major changes within the organization's operating environment or on recommendations provided by internal/ external auditors.

Policy Compliance

Compliance to the data privacy policy shall be reviewed on an annual basis by Head-IT to ensure continuous compliance monitoring through the implementation of compliance measurements and periodic review processes. For proactive detection of data breaches, please refer to breach management policy.

In cases where non-compliance is identified, Head-IT shall review the reasons for such non-compliance along with a plan for remediation and report them to Management. Depending on the conclusions of the review, the need for a revision to the policy may be identified. In instances of persistent non-compliance by the individuals concerned, they shall be subject to action in accordance with the PI Disciplinary Policy.

Data Privacy Principles

This Policy describes generally acceptable privacy principles (GAPP) for the protection and appropriate use of personal information at PI. These principles shall govern the use, collection, disposal, and transfer of personal information, except as specifically provided by this Policy or as required by applicable laws:

- **Notice**: PI shall provide data subjects with notice about how it collects, uses, retains, and discloses personal information about them.
- **Choice and Consent**: PI shall give data subjects the choices and obtain their consent regarding how it collects, uses, and discloses their personal information.
- **Rights of Data subject**: PI shall provide individuals with the right to control their personal information, which includes the right to access, modify, erase, restrict, transmit, or object to certain uses of their information and for withdrawal of earlier given consent to the notice.

- **Collection**: PI shall collect personal information from data subjects only for the purposes identified in the privacy notice / SoW / contract agreements and only to provide requested product or service.

- **Use, Retention and Disposal**: PI shall only use personal information that has been collected for the purposes identified in the privacy notice / SoW / contract agreements and in accordance with the consent that the data subject shall provide. PI shall not retain personal information longer than is necessary to fulfil the purposes for which it was collected and to maintain reasonable business records. PI shall dispose the personal information once it has served its intended purpose or as specified by the data subject.

- **Access**: PI shall allow data subjects to make inquiries regarding the personal information about them, that PI shall hold and, when appropriate, shall provide access to their personal information for review, and/or update.

- **Disclosure to Third Parties**: PI shall disclose personal information to Third Parties / partner firms only for purposes identified in the privacy notice / SoW / contract agreements. PI shall disclose personal information in a secure manner, with assurances of protection by those parties, according to the contracts, laws and other segments, and, where needed, with the consent of the data subject.

- **Obligations for Sub-processor**: Where a processor (vendor or 3rd party acting on behalf of PI's data processor) engages another processor (Sub-processor) for carrying out specific processing activities on behalf of PI (controller), the same data protection obligations as set out in the contract or other legal act between PI and the processor shall be imposed on the Sub-processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of GAPP. Where the Sub-processor fails to fulfil its data protection obligations, the initial processor (relevant vendor or 3rd party acting on behalf of PI's data processor) shall remain fully liable to PI for the performance of that Sub-processor's obligations.

- **Security for Privacy**: PI shall protect personal information from unauthorized access, data leakage and misuse.

- **Quality**: PI shall take steps to ensure that personal information in its records is accurate and relevant to the purposes for which it was collected.

- **Monitoring and Enforcement**: PI shall monitor compliance with its privacy policies, both internally and with Third Parties, and establish the processes to address inquiries, complaints, and disputes.

Notice

Notice shall be made readily accessible and available to data subjects before or at the time of collection of personal information or otherwise, notice shall be provided as soon as practical thereafter. Notice shall be displayed clearly and conspicuously and shall be provided online (e.g. by posting it on the intranet portal, website, sending mails, newsletters, etc.) and / or offline methods (e.g. through posts, couriers, etc.). All the web sites (including Intranet portals.

Collection of Personal Information

Personal information may be collected online or offline. Regardless of the collection method, the same privacy protection shall apply to all personal information.

- Personal information shall not be collected unless either of the following is fulfilled:
  - The data subject has provided a valid, informed, and free consent.

  - processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering a contract.
  - processing is necessary for compliance with the organization’s legal obligation.
  - processing is necessary to protect the vital interests of the data subject; or
  - processing is necessary for the performance of a task carried out in the public interest.

- Data subjects shall not be required to provide more personal information than is necessary for the provision of the product or service that data subject has requested or authorized. If any data not needed for providing a service or product is requested, such fields shall be clearly labelled as optional. Collection of personal information shall be avoided or limited when reasonably possible.
- Personal information shall be de-identified when the purposes of data collection can be achieved without personally identifiable information, at reasonable cost.
- When using vendors to collect personal information on the behalf of PI, it shall ensure that the vendors comply with the privacy requirements of PI as defined in this Policy.
- PI shall at minimum, annually review and monitor the information collected, the consent obtained and the notice / SoW / contract agreement identifying the purpose.
- The project team/support function shall obtain approval from the Head-IT before adopting the new methods for collecting personal information electronically.
- PI shall review the privacy policies and collection methods of Third Parties before accepting personal information from Third-Party data sources.

Use, Retention and Disposal

- Personal information may only be used for the purposes identified in the notice / SoW / contract agreements and only if the data subject has given consent.
- Personal information shall be retained for as long as necessary for business purposes identified in the notice / SoW / contract agreements at the time of collection or subsequently authorized by the data subjects.
- When the use of personal information is no longer necessary for business purposes, a method shall be in place to ensure that the information is destroyed in a manner sufficient to prevent unauthorized access to that information or is de-identified in a manner sufficient to make the data non-personally identifiable.
- PI shall have a documented process to communicate changes in retention periods of personal information required by the business to the data subjects who are authorized to request those changes.
- Personal information shall be erased if their storage violates any of the data protection rules or if knowledge of the data is no longer required by PI or for the benefit of the data subject. Additionally, PI has the right to retain the personnel information for legal and regulatory purposes and as per applicable data privacy laws.
- PI shall perform an internal audit on an annual basis to ensure that personal information collected is used, retained and disposed-off in compliance with the organization’s data privacy policy.

Access

PI shall establish a mechanism to enable and facilitate exercise of data subject's rights of access, blockage, erasure, opposition, rectification, and, where appropriate or required by applicable law, a system for giving notice of inappropriate exposure of personal information.

- Data subjects shall be entitled to obtain the details about their own personal information upon a request made and set forth in writing. PI shall provide its response to a request within 7 working days of receipt of written request.
- The data subjects shall have the right to require PI to correct or supplement erroneous, misleading, outdated, or incomplete personal information.
- Requests for access to or rectification of personal information shall be directed at the data subject's option, to the manager of the projects team or support function responsible for the personal information.
- The privacy coordinators shall record and document each access request as it is received, and the corresponding action taken.
- PI shall provide personal information to the data subjects in a plain simple format which is understandable (not in any code format).

Disclosure to Third Parties

Data Subject shall be informed in the privacy notice / SoW / contract agreement, if personal information shall be disclosed to Third Parties / partner firms, and it shall be disclosed only for the purposes described in the privacy notice / SoW / contract agreements and for which the data subject has provided consent.

- Personal information of data subjects may be disclosed to the Third Parties / partner firms only for reasons consistent with the purposes identified in the notice / SoW / contract agreements or other purposes authorized by law.
- PI shall notify the data subjects prior to disclosing personal information to Third Parties / partner firms for purposes not previously identified in the notice / SoW / contract agreements.
- PI shall communicate the privacy practices, procedures and the requirements for data privacy and protection to the Third Parties / partner firms.
- The Third Parties shall sign a NDA (Non-Disclosure Agreement) with PI before any personal information is disclosed to the Third Parties partner firms. The NDA shall include the terms on non-disclosure of customer information.

Security

Information security policy and procedures shall be documented and implemented to ensure reasonable security for personal information collected, stored, used, transferred and disposed by PI.

- Information asset labelling and handling guidelines shall include controls specific to the storage, retention and transfer of personal information.
- PI shall establish procedures that maintain the logical and physical security of personal information.
- PI shall establish procedures that ensure protection of personal information against accidental disclosure due to natural disasters and environmental hazards.

- Incident response protocols are established and maintained in order to deal with incidents concerning personal data or privacy practices.

- Individuals noticing or becoming aware of any breach of personal data shall notify the Head-IT within 2 hours. It shall be the Head-IT responsibility to analyses and act on the intimation of the same within 2 working days; furthermore, in accordance with low and/or comply policy.

Quality

PI shall maintain data integrity and quality, as appropriate for the intended purpose of personal data collection and use and ensure data is reliable, accurate, complete, and current.

- For this purpose, the data privacy officer and privacy coordinators shall have systems and procedures in place to ensure that personal information collected is accurate and complete for the business purposes for which it is to be used.

- PI shall perform an annual assessment on the personal information collected to check for accuracy, completeness, and relevance of the personal information.

Monitoring and enforcement

❖ **Dispute Resolution and Recourse**

PI shall define and document an Incident and policy which addresses privacy related incidents and breaches.

- The incident program includes a clear escalation path up to the executive management, legal counsel, and the board based on type and/or severity of the privacy incident/breach. It shall define a process to register all the incidents/complaints and queries related to data privacy.

- PI shall perform a periodic review of all the complaints related to data privacy to ensure that all the complaints are resolved in a timely manner and resolutions are documented and communicated to the data subjects.

- An escalation process for unresolved complaints and disputes which shall be designed and documented.

- Communication of privacy incident / breach reporting channels and the escalation matrix shall be provided to all the data subjects.

❖ **Dispute Resolution and Escalation Process for Employees**

Employees with inquiries or complaints about the processing of their personal information shall first discuss the matter with their immediate supervisor. If the employee does not wish to raise an inquiry or complaint with an immediate manager, or if the manager and employee are unable reach a satisfactory resolution of the issues raised, the employee shall bring the issue to the attention of the Head-IT.

❖ **Dispute Resolution and Escalation Process for Customer / Third Party**

Customers / Third Party with inquiries or complaints about the processing of their personal information shall bring the matter to the attention of the Head-IT Plasser India in writing. Any disputes concerning the processing of the personal information of non-employees shall be resolved through as per low or mutual consent.

❖ **Compliance Review**

An annual review will be done and reported to the management of PI.

Glossary

Term	**Definition**
Data Subject	A data subject who is the subject of personal and sensitive personal data.
Personal data or Personally Identifiable Information (PII)	PII is any information about an individual (the data subject) which can. • any information that can be used to distinguish or trace an individual 's identity. • any other information that is linked or linkable to an individual. Examples included but not limited to: Name, Address, Date of birth etc.
sensitive Personal Information (SPI)	Sensitive personal data means personal data consisting of information but not limited to the following attributes of the data subject: • 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. • genetic or biometric information. • racial and ethical origin. • political opinions. • religious or philosophical beliefs. • trade union membership. • any detail relating to the above clauses as provided to body corporate for providing service; and • 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 IT Act, 2008 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.
Third Party	All external parties – contractors, interns, summer trainees, vendors – who have access to PI information assets or information systems.
Data protection and security	Anyone collecting personal and customer information must fairly and lawfully process it, process it only for limited, specifically stated purposes, use the information in a way that is adequate, relevant and not excessive, use the information accurately, keep the information on file no longer than absolutely necessary, process the information in accordance with your legal rights, keep the information secure and never transfer the information outside the country without adequate protection

8. Relevant documents incl. guidelines, laws, standards and regulations	
EC Directives, as applicable	-
Statutory & Regulatory requirements	-
Standards (National & International)	ISO 27001:2013
Internal documents (Procedures / work instruction etc.)	PL-C-IT-29

9. Attachments *(Documents/Records)*	

End of Document