- Consequences of not providing the requested information.

7. Choice and consent

Choice refers to the options the data subjects are offered regarding the collection and use of their personal information. Consent refers to their agreement to the collection and use, often expressed by the way in which they exercise a choice option.

- N2S shall establish systems for the collection and documentation of data subject consents to the collection, processing, and/or transfer of personal data.
- Data subjects shall be informed about the choices available to them with respect to the collection, use, and disclosure of personal information.
- Consent shall be obtained (in writing or electronically) from the data subjects before or at the time of collecting personal information or as soon as practical thereafter.
- The changes to a data subject's preferences shall be managed and documented. Consent or withdrawal of consent shall be documented appropriately.
- The choices shall be implemented in a timely fashion and respected. If personal information is to be used for purposes not identified in the notice / SoW / contract agreements at the time of collection, the new purpose shall be documented, the data subject shall be notified, and consent shall be obtained prior to such new use or purpose.
- The data subject shall be notified if the data collected is used for marketing purposes, advertisements, etc.
- N2S shall review the privacy policies of the Third Parties and types of consent of Third Parties before accepting personal information from Third-Party data sources.

8. 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 in order to take steps at the request of the data subject prior to entering into a contract;
    - processing is necessary for compliance with the organizations legal obligation;
    - processing is necessary in order 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 N2S, it shall ensure that the vendors comply with the privacy requirements of N2S as defined in this Policy.
- N2S 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 IT Security team before adopting the new methods for collecting personal information electronically.
- N2S shall review the privacy policies and collection methods of Third-Parties before accepting personal information from Third-Party data sources.

9. 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.
- N2S 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 N2S or for the benefit of the data subject.

Additionally, N2S has the right to retain the personnel information for legal and regulatory purpose and as per applicable data privacy laws.

- N2S 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.

10. Access

N2S 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. N2S shall provide its response to a request within 72 hours of receipt of written request.
- The data subjects shall have the right to require N2S 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 members of the compliance team shall record and document each access request as it is received and the corresponding action taken.
- N2S shall provide personal information to the data subjects in a plain simple format which is understandable (not in any code format).

11. 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.
- N2S 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.

- N2S 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 N2S before any personal information is disclosed to the Third Parties partner firms. The NDA shall include the terms on non-disclosure of customer information.

12. 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 N2S.

- Information asset labelling and handling guidelines shall include controls specific to the storage, retention and transfer of personal information.
- Management shall establish procedures that maintain the logical and physical security of personal information.
- Management 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.

13. Quality

N2S 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 general counsel and the compliance team 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.
- N2S shall perform an annual assessment on the personal information collected to check for accuracy, completeness and relevance of the personal information.

14. Monitoring and enforcement

14.1. Dispute Resolution and Recourse

N2S shall define and document an Incident and Breach Management policy which addresses the privacy related incidents and breaches.

- The incident and breach management 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
- N2S 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.

14.2. 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 to reach a satisfactory resolution of the issues raised, the employee shall bring the issue to the attention of the General Counsel.

14.3. 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 General Counsel in writing. Any disputes concerning the processing of the personal information of non-employees shall be resolved through arbitration.

14.4. Compliance Review

Compliance Team shall conduct an internal audit annually (at minimum) to ensure compliance with the established privacy policies and applicable laws.

- The internal audit shall consist of the review of the following:
  - personal information collected from data subjects;
  - the purposes of the data collection and processing;
  - the actual uses of the data;
  - disclosures made about the purposes of the collection and use of such data;

- the existence and scope of any data subject consents to such activities;
- any legal obligations regarding the collection and processing of such data, and
- the scope, sufficiency, and implementation status of security measures.

- The Compliance team shall document all the instances of non-compliance with privacy policies and procedures and report the same with the Data Privacy Management committee.
- The General Counsel along with the Compliance Team shall take actions on the findings from the internal audit and work on the recommendations for improvement of the privacy posture
- Any changes made to the policies shall be communicated to all the employees, the stakeholders and the customers / clients.

15. 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 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.
Third Party	All external parties – contractors, interns, summer trainees, vendors – who have access to N2S 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

Term	Definition
	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