Data Privacy Policy

Version: 1.0

Contents

1. Data Privacy Policy

1.1. Objective

The purpose of this policy is to maintain the privacy of and protect the sensitive personal information of employees, contractors, vendors, interns, associates, customers and business partners of Tata BlueScope Steel Private Limited and to ensure the compliance with laws and regulations applicable to Tata BlueScope Steel Private Limited (hereafter referred to as "TBSPL" or "the organization").

1.2. Scope

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

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

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

1.3. Responsibilities/ Implementation

The owner for the Data Privacy Policy shall be the Grievance Officer. The Data Privacy Officer shall be responsible for maintenance and accuracy of this policy. Any queries regarding the implementation of this Policy shall be directed to the Grievance Officer.

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

1.4. Policy Compliance

Compliance to the data privacy policy shall be reviewed on an annual basis by Human Resource team to ensure continuous compliance monitoring through the implementation of compliance measurements and periodic review processes.

In cases where non-compliance is identified, the Data Privacy officer/ Grievance Officer shall review the reasons for such non-compliance along with a plan for remediation and report them to Human Resource Team. Depending on the conclusions of the review, 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 disciplinary action, which Grievance Officer finds appropriate.

1.5. Data Privacy Principles

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

- **Notice:** TBSPL shall provide data subjects with notice about how it collects, uses, retains, protects and discloses sensitive personal information about them.

- **Choice and Consent:** TBSPL shall give data subjects the choices and obtain their written consent regarding how it collects, uses, and discloses their sensitive personal information.

- **Rights of Data subject/s:** TBSPL shall provide individuals with the right to control their sensitive personal information, which includes the right to access, modify, erase, restrict, transmit, or object to certain uses of their sensitive personal information and for withdrawal of earlier given consent to the notice.

- **Collection:** TBSPL shall collect personal information from data subjects only for the lawful purposes identified in the privacy notice / SoW / contract / agreements and only to provide or receive requested product or service. TBSPL shall also collect, retain and transfer sensitive personal information to meet any requirement of the applicable statute or to comply with any order, instructions, directions etc. of the judicial, quasi-judicial, local administration, police or any authority duly empowered to collect such sensitive personal information.

- **Use, Retention and Disposal:** TBSPL shall only use sensitive personal information that has been

collected for the lawful purposes identified in the privacy notice / SoW / contract/ agreements and in accordance with the consent that the data subject shall provide. TBSPL shall not retain sensitive personal information longer than is necessary to fulfil the lawful purposes for which it was collected and to maintain reasonable business records. TBSPL shall dispose the sensitive personal information once it has served its intended lawful purpose or as specified bythe data subject/s. TBSPL or any authorized person acting on behalf of TBSPL has no responsibility for anything whatsoever, direct or indirect, if sensitive personal information is found to be misleading, false and inaccurate.

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

- **Disclosure to Third Parties:** TBSPL shall disclose sensitive personal information to Third Parties /partner firms only for lawful purposes identified in the privacy notice / SoW / contract/ agreements. TBSPL shall disclose sensitive 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 consent of the data subject. TBSPL may require to disclose sensitive personal information under any applicable statute or to comply any with order, instructions, directions etc. of the judicial, quasi-judicial, local administration, police or any authority duly empowered in this behalf.

- **Obligations for Sub-processor:** Where a processor (vendor or 3rd party acting on behalf of TBSPL's data processor) engages another processor (Sub-processor) for carrying out specific processing activities on behalf of TBSPL (controller), the same data protection obligations as set out in the contract or other legal act between TBSPL 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 the applicable law. Where the Sub-processor fails to fulfil its data protection obligations, the initial processor (relevant vendor or 3rd party acting on behalf of TBSPL's data processor) shall remain fully liable and keep indemnified TBSPL for the performance of that Sub- processor's obligations.

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

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

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

1.6. Notice

Notice shall be made readily accessible and available to data subjects before or at the time of collection of sensitive personal information or otherwise, notice shall be provided as soon as practical thereafter. Notice shall be displayed clearly and conspicuously and shall be provided through 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), and any product or service that collects sensitive personal information internally, shall have a privacy notice. In case of any cross-border transfer of sensitive personal information, the data subjects shall be informed by a notice sufficiently prior to the transfer and the data subjects shall have right to not give consent for the said transfer.

Privacy notices may include:

- the organization's operating jurisdictions; Third Parties involved; business segments and affiliates; lines of business; locations;
- types of sensitive personal information collected; sources of sensitive personal information; who is collecting the sensitive personal information, including contact information;
- the purpose of collecting the sensitive personal information;
- assurance that the sensitive personal information will be used only for the purpose identified in the notice and only if the implicit and / or explicit consent is provided unless a law or regulation specifically requires otherwise;
- any choices the data subject/s have regarding the use or disclosure of the sensitive personal information;
- the process data subject/s shall follow to exercise the choices;
- the process for a data subject to change contact preferences and ways in which the consent is obtained.
- collection process and how the sensitive personal information is collected; how the information is used including any onward transfer to Third-Parties;
- retention and disposal process for sensitive personal information; assurance that the sensitive personal information to be retained only as long as necessary to fulfill the stated lawful purposes, or for a period specifically required by law or regulation and will be disposed-off

securely or made anonymous post the identified purpose is completed;

- process of accessing sensitive personal information; the costs associated for accessing sensitive personal information (if any); process to update / correct the sensitive personal information; the resolution of disagreements related to sensitive personal information; how the sensitive personal information is protected from unauthorized access or use;
- how users will be notified of any changes made to privacy notice;
- disclosure process for Third Parties; the assurance that the sensitive personal information is disclosed to Third Parties only for the lawful purpose identified; the remedial actions in place for any misuse of sensitive personal information by the Third Parties;
- security measures in place to protect the sensitive personal information; ways of maintaining quality of sensitive personal information;
- monitoring and enforcement mechanisms in place; description of the complaint channels available to data subjects; how the internal personnel, key stakeholders and the customers can contact the Company related to any privacy complaints or breaches; relevant contact information and / or other reporting methods through which the complaints and/or breaches could be registered;
- Consequences of not providing the requested information.

1.7. Choice and consent

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

- TBSPL shall establish systems for the collection and documentation of data subject/s consents to the collection, processing, and/or transfer of sensitive personal information and data.
- Data subjects shall be informed about the choices available to them with respect to the collection, use, and disclosure of sensitive personal information.
- Consent shall be obtained (in writing or electronically) from the data subjects before or at the time of collecting sensitive 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 sensitive personal information is to be used for the 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.

- Data subject represents and warrants that sensitive personal information furnished is true and accurate and Data subject shall indemnify and keep indemnified TBSPL against any losses, claims, damages, costs, proceedings, liabilities arising out of or in connection with false, misleading and inaccurate sensitive personal information furnished by Data subject.
- TBSPL shall review the privacy policies of the Third Parties and types of consent of Third Parties before accepting sensitive personal information from Third-Party data sources.

1.8. Collection of Sensitive Personal Information

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

- Sensitive Personal information shall not be collected unless either of the following is fulfilled:
  - the data subject/s has provided a valid, informed and free consent ;
  - processing is necessary for the performance of a SOW/agreement/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 organization's legal obligation;
  - processing is necessary in order to protect the vital interests of the data subject/s; 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 sensitive personal information than is necessary for the provision of the product or service that data subject has requested or authorized or for the purpose specified in the notice.
- Sensitive personal information shall be de-identified when the purposes of data collection can be achieved without personally identifiable information, at reasonable cost.
- When using any authorized third party to collect sensitive personal information on the behalf of TBSPL, it shall ensure that the third party comply with the privacy requirements of TBSPL as defined in this Policy.
- TBSPL shall at minimum, annually review and monitor the sensitive personal 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 of the organization before adopting the new methods for collecting, usage, retention and transferof sensitive personal information electronically.
- TBSPL shall review the privacy policies and collection methods of Third-Parties before accepting sensitive personal information from Third-Party data sources.

1.9. Use, Retention and Disposal

- Sensitive personal information may only be used for the purposes identified in the notice / SoW / contract/ agreements and only if the data subject/s has given consent. The consent is dispensed with if sensitive personal information is used for fulfilling TBSPL's legal obligation;
- Sensitive personal information shall be retained for as long as necessary for lawful purposes identified in the notice / SoW / contract/ agreements at the time of collection or subsequently authorized by the data subjects.

- When the use of sensitive personal information is no longer necessary for lawful business purposes, a method shall be in place to ensure that the sensitive personal information is destroyed in a manner sufficient to prevent unauthorized access to that sensitive personal information or is de-identified in a manner sufficient to make the data non-personally identifiable.
- TBSPL shall have a documented process to communicate changes in retention periods of sensitive personal information required by the business to the data subjects who are authorized to request those changes.
- Sensitive 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 TBSPL or for the benefit of the data subject. Additionally, TBSPL has the right to retain the sensitive personnel information for legal and regulatory purpose and as per applicable data privacy laws.
- TBSPL shall perform an internal audit on an annual basis to ensure that sensitive personal information collected is used, retained and disposed-off in compliance with the organization's data privacy policy.

1.10. Access

TBSPL 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 sensitive personal information.

- Data subjects shall be entitled to obtain the details about their own sensitive personal information upon a request made and set forth in writing. TBSPL shall provide its response to a request within 72 hours of receipt of written request.
- The data subjects shall have the right to require TBSPL to correct or supplement erroneous, misleading, outdated, or incomplete sensitive personal information.
- Requests for access to or rectification of sensitive personal information shall be directed, at the data subject's option, to the manager of the projects team or support function responsible for the sensitive personal information.

- The privacy coordinators shall record and document each access request as it is received and the corresponding action taken.
- TBSPL shall provide sensitive personal information to the data subjects in a plain simple format which is understandable (not in any code format).

1.11. Disclosure to Third Parties

Data Subject shall be informed in the privacy notice / SoW / contract/ agreement, if sensitive 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.

- Sensitive 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.
- TBSPL shall notify the data subjects prior to disclosing sensitive personal information to Third Parties / partner firms for purposes not previously identified in the notice / SoW / contract/ agreements.
- TBSPL 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 TBSPL before any sensitive personal information is disclosed to the Third Parties partner firms. The NDA shall include the terms on non-disclosure of customer information.

1.12. Security

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

- Information asset labelling and handling guidelines shall include controls specific to the storage, retention and transfer of sensitive personal information.
- Management shall establish procedures that maintain the logical and physical security of sensitive personal information.
- Management shall establish procedures that ensure protection of sensitive 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 sensitive personal information and data or privacy practices.
- IT team shall exercise periodically the review of information security safeguards and in-built

mechanism for the collection, use, protection and transfer of sensitive personal information as envisaged in this policy.

1.13. Quality

TBSPL shall maintain data integrity and quality, as appropriate for the intended purpose of sensitive personal information /data collection and use and also ensure that data is reliable, accurate, complete and current.

- For this purpose, the Grievance Officer and IT Security team shall have systems and procedures in place to ensure that sensitive personal information collected is accurate and complete for the lawful business purposes for which it is to be used.
- TBSPL shall perform an annual assessment on the sensitive personal information collected to check for accuracy, completeness and relevance of the sensitive personal information.

1.14. Monitoring and enforcement

1.14.1. Dispute Resolution and Recourse

Grievance Officer is Ms. Meenakshi Nayyar, Legal Head and Company Secretary or any other officer authorized by the Company from time to time and displayed on the Company's website from time to time. The Grievance Officer shall address the privacy related incidents and breaches.

- TBSPL 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.
- Data subjects can also communicate their grievances through Whistle Blower mechanism.

1.14.2. Dispute Resolution and Escalation Process for Employees

Employees with inquiries or complaints about the processing of their sensitive 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 unableto reach a satisfactory resolution of the issues raised, the employee shall bring the issue to the attention of the Grievance Officer. (Emailing at 11eenakshi.nayyar@tatabluescopesteel.com).

1.14.3. Dispute Resolution and Escalation Process for Customer / Third Party

Customers / Third Party with inquiries or complaints about the processing of their sensitive personal information shall bring the matter to the attention of the Grievance Officer in writing and Grievance officer shall resolve the same as per applicable laws and rules thereunder.

1.14.4. Enforcement and Compliance Review

Human Resource Team and Information Technology Team shall be jointly responsible for the compliance and execution of this Privacy Policy with respect to its respective responsibilities. Human Resource Team in collaboration with Information Technology 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:
    - Sensitive personal information collected from data subjects;
    - the purposes of the sensitive personal information/ data collection and processing;
    - the actual uses of the sensitive personal information / data;
    - disclosures made about the purposes of the collection and use of such sensitive personal information/ data;
    - the existence and scope of any data subject consents to such activities;
    - any legal obligations regarding the collection and processing of such sensitive personal information / data, and
    - the scope, sufficiency, and implementation status of security measures.
- Human Resource team shall document all the instances of non-compliance with privacy policies and procedures and report the same with the Grievance Officer.
- The Grievance Officer 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.

2. Glossary

Term	Definition
Data Subject	A data subject who is the subject of sensitive personal information /data.
Personal data or Personally Identifiable Information (PII)	PII is any information about an individual (the data subject) which may be • any information/ data that can be used to distinguish or capable of identifying an individual's identity; • any other information/ data that is linked or linkable to an individual Examples included but not limited to: Name, Address, Date of birth, medical records, pan card, Aadhar card, passport, sexual orientation etc.
Sensitive Personal Information/ Data (SPI)	Sensitive personal information/ 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' viz. contractors, interns, trainees, vendors etc. who have access to TBSPL information assets and/or information systems.
Data protection and security guidelines	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

Prepared by:	Recommended by:	Approved by:
Meenakshi Nayyar **Legal Head & Company Secretary**	**Anita Panakkal** **Chief – HR & IR**	**Riten Choudhury** **Managing Director**
SD/-	SD/-	SD/-