Date of Start	Privacy and Personal Data Protection Policy	Code	Policy- R-GEN23
03-June-2025		Responsible	IT
		Department in charge	Administration – IT

Article 01 Objective:

- To establish a framework for safeguarding the privacy and security of Personally Identifiable Information (PII) processed by TDS Lithium-Ion Battery Gujarat Pvt. Ltd. (TDSG). This framework aims to ensure that PII is protected in accordance with applicable legal, regulatory, and organizational requirements concerning PII.

Article 02 Scope:

- This policy applies to all internal and external stakeholders of TDSG.

Article 03 Definitions of terms:

1. **Personally Identifiable Information (PII)**: Any information that can be used to identify a specific person, such as their name, address, phone number, email and sensitive information like bank details.
2. **Processing**: Any action taken with personal data, like collecting, storing, using, or sharing it.

Article 04 Principles Relating to collection and Processing of Personal Data:

1. **Processed lawfully, fairly, and transparently:**
   TDSG ensures personal data is handled only with a clear legal basis and by informing individuals about how their information is used.

2. **Collected for specified, legitimate purposes and not further processed in ways incompatible with those purposes:**
   Personal data at TDSG is gathered for distinct, valid reasons (e.g., HR, order processing) and is not used for unrelated activities without proper justification or consent.

3. **Adequate, relevant, and limited to what is necessary for the purposes of processing:**
   TDSG collects and processes only the essential personal data required to achieve its specific operational objectives, avoiding the collection of excessive information.

4. **Accurate and kept up-to-date:**
   TDSG shall maintain personal data accuracy through regular reviews, promptly updates when new information is received, and by enabling individuals to request necessary corrections.

5. **Retained only for as long as necessary for processing purposes:**
   TDSG retains personal data largely without a formal retention schedule, keeping it for operational continuity and historical reference, rather than strictly limiting storage duration to the necessity defined by specific processing purposes or legal mandates.

6. **Processed securely to prevent unauthorized access, loss, destruction, or damage:**
   TDSG implements appropriate technical (Data loss prevention) and organizational security measures to safeguard personal data against breaches, ensuring its confidentiality and integrity throughout its operations.

Article 05 Rights of the Individual

The Individual has rights, including:

1. The right to be informed.
2. The right of access.
3. The right to rectification.
4. The right to erasure.
5. The right to restrict processing.
6. The right to data portability.
7. The right to object.
8. Rights concerning automated decision-making and profiling.

Article 06 Consent:

- Where consent is required for processing personal data, TDSG shall explicitly obtain consent, especially when processing the data of Employee, Vendor/Customer and any third party. The consent must be clear, informed, and capable of being withdrawn at any time.

Article 07 Personal Data Breach Notification:

This section outlines the policy to be followed in the event of a personal data breach. A personal data breach can include incidents such as unauthorized access, accidental disclosure, or the destruction of personal data. The personal data breaches that are likely to result in risks to the rights of individuals shall be reported to the relevant authority within the stipulated time.

Article 08 Breach Notification Process:

- There are three parties that may need to be notified in the event of a personal data breach:
    1. **Notification to the Relevant Authorities**: In the event of a breach, appropriate authorities (Board of Directors, Senior Management just below the Board of Directors, Information security officer and other relevant stakeholders) shall inform promptly to Govt. bodies & statutory bodies, as required by applicable laws and regulations, unless the breach is unlikely to pose any risk to individuals.

    2. **Notification to Affected Individuals**: If the breach is likely to result in significant risks to individuals' rights or those affected shall be informed on an immediate basis with clear guidance on mitigating potential impacts.

    3. **Internal Reporting and Communication**: The incident shall be reported internally to designated roles, Compliance Committee members, Information security committee members and Top Management ensuring swift action and documentation of the response.

Article 09 Security Practise and Procedures for PII Handling:

- To ensure the secure handling of Personally Identifiable Information (PII), TDSG has established the following policy **Data should be stored in a secure way** during transmission and while stored to ensure data confidentiality, Integrity, and Availability.

This applies to all sensitive information, such as employee records, customer details, and financial data.

1. **Access Control**: Access to PII is granted only to authorized individuals whose roles require such access. Regular audits shall be conducted to ensure compliance, and access rights will be reviewed periodically.

2. **Anonymization and Pseudonymization**: Where feasible, PII shall be anonymized or pseudonymized, particularly for research, analytics, or external sharing. This reduces the risk of identifying individuals if data is compromised.

3. **Data Retention**: PII shall be retained only for as long as necessary to fulfill its intended purpose or to meet legal and regulatory requirements rather than strictly limiting storage duration to the necessity defined by specific processing purposes or legal mandates.

4. **Regular Audits and Training**: Regular audits shall be conducted to ensure compliance with data protection laws. All employees shall receive training on secure data handling practices and the importance of protecting PII.

5. **Incident Response**: A detailed incident response plan is in place to handle potential data breaches. This includes procedures for containment, investigation, notification, and mitigation.

6. **Secure Data Sharing**: Any PII shared with third parties shall be protected through secure communication channels (Emails, MS Teams). Third parties should also be required to comply with TDSG's data protection policies.

Article 10 Compliance:

- This policy complies with Information Technology Act, 2000. And TDSG will periodically review and update this policy to ensure it remains in compliance with any changes in legislation.

Article 11 Grievance Redressal Mechanism:

TDSG has appointed Grievance Officer for the purposes of addressing grievances related to data privacy in accordance with IT Act, 2000, and will be responsible for receiving, investigating, and redressing such concerns to uphold individuals' data privacy rights.

Any relevant complaint must be addressed to the Grievance Officer in writing with necessary details and evidence. The relevant email ID for the purpose is grievance@Tdsgj.co.in

REVISION HISTORY

Version	Date of release	Summary of changes
v1	03-June-2025	Policy Introduced