AventIQ, a trademark of Mittal Software Labs Limited.

Data Protection and Privacy Policy
Confidential and Restricted

Objective

AventIQ, a trademark of Mittal Software Labs Limited. is committed to protecting the personal and sensitive data of its employees, clients, and business partners. This policy ensures that data is collected, processed, stored, and shared in a secure and lawful manner in compliance with applicable Indian laws, including the Information Technology Act, 2000, and emerging frameworks like the Digital Personal Data Protection Act, 2023.

Scope and Applicability

This policy applies to all employees, contractors, interns, and third-party vendors engaged with AventIQ. It governs the handling of personal data in both physical and electronic formats.

Key Definitions:

1. **Personal Data**: Any information relating to an identified or identifiable individual (e.g., name, contact details, address, employment information).
2. **Sensitive Personal Data**: Data that includes financial information, health records, biometric data, and passwords.
3. **Processing**: Any operation performed on data, such as collection, recording, storage, retrieval, sharing, or deletion.
4. **Data Subject**: An individual whose personal data is being processed by AventIQ.
5. **Data Controller**: AventIQ, as the entity determining the purpose and means of processing personal data.
6. **Data Processor**: Any third-party vendor authorized to process personal data on behalf of AventIQ.

Policy Principles

1. **Lawfulness, Fairness, and Transparency**:
    - Data must be processed lawfully, fairly, and transparently.

    - Individuals must be informed about how their data is collected, used, and stored.

2. **Purpose Limitation**:
    - Data shall only be collected for specific, explicit, and legitimate purposes and not processed further in a manner incompatible with those purposes.
3. **Data Minimization**:
    - Only the data necessary for the intended purpose will be collected and retained.
4. **Accuracy**:
    - AventIQ shall ensure that personal data is accurate and kept up-to-date.
5. **Storage Limitation**:
    - Data shall not be retained for longer than necessary, unless required for legal or contractual obligations.
6. **Integrity and Confidentiality**:
    - Appropriate technical and organizational measures will be implemented to ensure data security and prevent unauthorized access, loss, or misuse.
7. **Accountability**:
    - AventIQ is responsible for demonstrating compliance with this policy.

Data Collection and Processing

1. **Consent**:
    - Explicit consent shall be obtained from individuals before collecting their personal or sensitive data, except where processing is required by law.
2. **Notice**:
    - Data subjects will be informed about the purpose of data collection, retention period, and their rights.
3. **Third-Party Processing**:
    - Contracts with data processors shall include data protection obligations to ensure compliance with this policy.
4. **Cross-Border Data Transfers**:

- Personal data shall not be transferred outside India unless adequate safeguards are in place and permitted by applicable laws.

Rights of Data Subjects

1. **Right to Access**:
    - Individuals can request access to their personal data and obtain information about how it is processed.
2. **Right to Rectification**:
    - Individuals may request corrections to inaccurate or incomplete data.
3. **Right to Erasure**:
    - Individuals may request the deletion of their data, subject to legal and contractual obligations.
4. **Right to Data Portability**:
    - Individuals may request their data in a structured, machine-readable format for transfer to another data controller.
5. **Right to Object**:
    - Individuals may object to data processing for direct marketing or other purposes.

Data Security Measures

1. **Access Control**:
    - Only authorized personnel shall have access to personal data based on their roles and responsibilities.
2. **Encryption**:
    - Sensitive personal data shall be encrypted during transmission and storage.
3. **Regular Audits**:
    - Periodic audits shall be conducted to ensure compliance with data protection practices.
4. **Incident Management**:

- A data breach response plan shall be in place to address and mitigate data breaches promptly.

Data Retention and Disposal

1. **Retention Period**:
    - Personal data shall be retained only for the duration necessary to fulfil its purpose or comply with legal requirements.
2. **Secure Disposal**:
    - Data no longer required shall be securely deleted or destroyed to prevent unauthorized access or recovery.

Non-Compliance and Penalties

1. Employees or third-party vendors found in violation of this policy shall face disciplinary action, up to and including termination of employment or contracts.
2. Legal actions may also be pursued for breaches under applicable data protection laws.

Legal Compliance

This policy complies with:

- The Information Technology Act, 2000.
- The Digital Personal Data Protection Act, 2023 (or equivalent enacted law).
- Relevant provisions under the Delhi Shops and Establishments Act, 1954.

Review and Amendments

This policy will be reviewed annually or upon significant legal or organizational changes to ensure compliance and relevance.

Approved By: Nikhil Mittal
Effective Date: 01-Jan-2025
Last Updated: 26-Dec-2024