ARYA FIN-TRADE SERVICES (INDIA) PRIVATE LIMITED

DATA PROTECTION, RETENTION & DISPOSAL POLICY

Version	**2024/01.02**
Review Date	**05/04/2024**
Review & Approved by	**Reviewed by Technology Committee & Approved by Board of Directors**

1. Policy Statement:

- The organization registered as a Stock Broker and Depository Participant recognizes the importance of appropriately Protecting, retaining and disposing of data in compliance with regulatory requirements.
- This policy establishes guidelines and procedures for the secure protection, retention and disposal of data to protect client information, maintain data integrity, and comply with applicable laws and regulations.

2. Data Protection:

a. Confidentiality and Access Control:

- Implement appropriate access controls, including user authentication, role-based access, and data encryption, to protect sensitive client data from unauthorized access.
- Regularly review and update access control mechanisms to ensure the confidentiality of data.

b. Integrity and Data Accuracy:

- Maintain data integrity by implementing controls to prevent unauthorized modifications, deletions, or alterations of data.
- Regularly validate and verify data accuracy through data validation checks and reconciliation processes.

c. Data Encryption:

- Utilize encryption techniques for sensitive data transmission and storage to protect against unauthorized interception or access.

d. Data Backup and Recovery:

- Regularly back up critical data and establish procedures for data recovery in the event of data loss or system failures.
- Test and verify the effectiveness of data backup and recovery processes periodically.

e. Data Minimization:

- Only collect and retain data that is necessary for business purposes and regulatory compliance.
- Implement measures to minimize the collection and storage of unnecessary data.

f. Incident Response:

- Develop an incident response plan to effectively address data breaches or security incidents.
- Establish procedures for reporting, investigating, and mitigating data breaches or unauthorized access incidents promptly.

g. Third-Party Data Handling:

- a. Establish agreements with third-party vendors and service providers to ensure they adhere to data protection and security standards.
- b. Conduct due diligence on third parties handling client data to assess their security controls and data protection practices.

3. Data Disposal:

- ➤ Identify data that is no longer needed for business or legal purposes and can be safely disposed of.
- ➤ Implement secure data disposal methods, such as shredding physical documents or using certified data destruction software for electronic media.
- ➤ Maintain records of the disposal process, including dates, methods used, and responsible individuals.

4. Data Retention:

- ➤ Determine data retention periods based on regulatory requirements, legal obligations, and business needs.
- ➤ Classify data based on its sensitivity and assign appropriate retention periods for each category.
- ➤ Develop a data retention schedule outlining the retention periods for different types of data.

List of Data Type and its retention periods:

Data Type	Description	Retention Period
Personal Identifiable Information (PII)	Data that directly or indirectly identifies an individual, including but not limited to name, address, contact details, Aadhaar number, PAN, bank account details, KYC documents, etc	Retain PII data as per SEBI guidelines and relevant regulatory requirements, typically for a minimum of 5 years after the closure of the client account or termination of the business relationship.
Financial and Trading Data	Data related to financial transactions, trading activities, investment portfolios, order details, transaction records, bank statements, trade confirmations, etc	Retain financial and trading data as per SEBI guidelines and applicable laws, typically for a minimum of 7 years from the transaction date or as required by specific regulations
Compliance and Audit Data	Data related to compliance activities, internal audits, regulatory audits, risk assessments, AML/CFT records, suspicious transaction reports (STRs), etc	Retain compliance and audit data as per SEBI guidelines and relevant regulatory requirements, typically for a minimum of 8 years from the date of creation or as specified by specific regulations.
Legal and Contractual Documents	Data related to legal agreements, contracts, agreements, power of attorneys, client agreements, non-disclosure agreements (NDAs), etc	Retain legal and contractual documents as per SEBI guidelines and applicable legal requirements, typically for the duration of the contract/agreement and a reasonable period thereafter as necessary for legal purposes.
Employee Records	Data related to employees, including employment contracts, personnel files, payroll records, performance evaluations, training records, etc.	Retain employee records as per SEBI guidelines, labor laws, and relevant legal requirements, typically for a minimum of 7 years after the employee's separation from the organization.
IT Logs and System Records	Data logs, system records, access logs, network logs, security event logs, incident response records, etc	Retain IT logs and system records as per SEBI guidelines and relevant legal requirements, typically for a minimum of 5 years or as specified by specific regulations.

Marketing and Communication Data	Data related to marketing activities, client communications, customer preferences, marketing analytics, customer surveys, etc.	Retain marketing and communication data as per SEBI guidelines and applicable marketing laws, typically for a reasonable period to support business and marketing efforts, and as required for legal compliance

5. Compliance with Regulatory Requirements:

a. Ensure data retention practices comply with applicable laws, regulations, and guidelines, including SEBI regulations and data protection laws.
b. Stay updated with changes in regulations and adjust data retention policies accordingly.

6. Secure Storage:

a. Store retained data in a secure manner, protecting it from unauthorized access, theft, or physical damage.
b. Implement access controls, encryption, and other security measures to safeguard retained data.

7. Data Retention Periods:

a. Document the specific retention periods for different types of data in the data retention schedule.
b. Consider factors such as legal requirements, statutory limitations, contractual obligations, and business needs when determining retention periods.
c. Review and update the retention periods periodically to ensure compliance with changing regulations and business requirements.

8. Data Destruction Procedures:

a. Develop procedures for securely disposing of data at the end of its retention period.
b. Clearly define the methods and tools to be used for data destruction, such as physical destruction, data wiping, or degaussing.
c. Ensure that responsible individuals follow the designated data destruction procedures consistently and maintain proper documentation.

9. Employee Training and Awareness:

a. Conduct regular training programs to educate employees about data protection best practices, including confidentiality, data handling, and security protocols. b. Foster a culture of data protection awareness and encourage employees to report any potential security vulnerabilities or breaches.
b. Provide training to employees on data disposal and retention policies, emphasizing their roles and responsibilities in **ensuring compliance.**
c. Raise awareness about the importance of data protection and the potential risks associated with improper data disposal or retention.

10. Monitoring:

a. Regularly monitor compliance with the data disposal and retention policy and review data disposal and retention practices to identify and address any non-compliance or gaps in the process.

11. Documentation and Recordkeeping:

a. Maintain accurate records of data disposal and retention activities, including disposal dates, methods used, and retention periods.
b. Keep records accessible for compliance verification, internal audits, and regulatory inspections.

12. Policy Review and Updates:

a. Review the Data Protection, Disposal and Data Retention Policy periodically to ensure its effectiveness, relevance, and compliance with changing regulations.
b. Update the policy as necessary to reflect new regulatory requirements or changes in business practices.