Supply Chain and Logistics Academy Pte Ltd ("SCALA")

Data Protection and Management Policy

1. Purpose

We at SCALA (the "Company") respect the privacy and confidentiality of the personal data of our Clients, Customers, Visitors, and others with whom we interact in the course of providing our services. We are committed to implementing policies, practices, and processes to safeguard the collection, use, and disclosure of personal data in compliance with the Singapore Personal Data Protection Act 2012 ("PDPA").

The purpose of this Data Protection Policy is to explain how the Company collects, uses, discloses, processes, and retains personal data, and to ensure compliance with applicable data protection laws and regulations.

2. Scope

This Data Protection Policy applies to all personal data collected, used, disclosed, processed, and retained by the Company in the course of its business operations. It covers the personal data of Clients, Customers, Visitors, employees, vendors, and any other individuals who interact with the Company.

As our business continues to evolve, this policy may be updated from time to time. Individuals are encouraged to review the policy periodically to stay informed of any changes.

3. Definitions

- **Personal Data**: Any information relating to an identified or identifiable natural person.
- **Sensitive Data**: Special categories of personal data, including but not limited to, racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, and data concerning sexual orientation.
- **Data Subject**: Any individual whose personal data is collected and processed by SCALA
- **Processing**: Any operation performed on personal data, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction.
- **Data Controller**: Management and staff of SCALA, which determines the purposes and means of processing personal data.
- **Data Processor**: Any person processing personal data, whether for SCALA or on behalf of SCALA
- **PDPA**: Personal Data Protection Act, Singapore's data protection law governing the collection, use, and disclosure of personal data.

- **Cloud Data Centre**: A virtualized storage facility used to store and manage data, hosted by third-party cloud service providers.

4. Data Protection Principles

SCALA adheres to the following principles when processing personal data:

1. **Lawfulness, Fairness, and Transparency**: Data must be processed lawfully, fairly and transparently.
2. **Purpose Limitation**: Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. **Data Minimisation**: Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
4. **Accuracy**: Data must be accurate and, where necessary, kept up to date.
5. **Storage Limitation**: Data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed.
6. **Integrity and Confidentiality**: Data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
7. **Accountability**: SCALA is responsible for, and must be able to demonstrate, compliance with these principles.

5. Data Subject Rights

SCALA recognizes and upholds the following rights of data subjects under PDPA and other applicable laws:

1. **Right to be Informed**: Data subjects have the right to be informed about the collection and use of their personal data.
2. **Right of Access**: Data subjects have the right to access their personal data and supplementary information.
3. **Right to Correction**: Data subjects have the right to have inaccurate personal data corrected or completed if it is incomplete.
4. **Right to Erasure**: Data subjects have the right to have their personal data erased in certain circumstances, also known as the "right to be forgotten."
5. **Right to Restrict Processing**: Data subjects have the right to request the restriction or suppression of their personal data.
6. **Right to Data Portability**: Data subjects have the right to obtain and reuse their personal data for their own purposes across different services.

7. **Right to Object**: Data subjects have the right to object to the processing of their personal data in certain circumstances.
8. **Rights in Relation to Automated Decision-Making and Profiling**: Data subjects have the right not to be subject to a decision based solely on automated processing, significantly affects them.

6. Data Collection and Use

SCALA will collect and use personal data only for legitimate business purposes and in a manner that is fair and lawful. This includes:

- **Consent**: Where required by law, SCALA will obtain the data subject's consent before collecting or processing personal data. Consent must be freely given, specific, informed, and unambiguous.
- **Legitimate Interests**: Processing may be based on the legitimate interests of SCALA, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subjects.
- **Contractual Necessity**: Personal data may be processed if it is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract.
- **Legal Obligation**: SCALA may process personal data where necessary to comply with a legal obligation; i.e. in the application of a registrant for SCALA programmes and in submission of grants.

7. Data Security

SCALA is committed to protecting personal data against unauthorized or unlawful processing and against accidental loss, destruction, or damage. We implement appropriate technical and organizational measures, including:

- **Access Controls**: Limiting access to personal data to authorized personnel only.
- **Encryption**: Using encryption technologies to protect data during transmission and storage, especially for data stored in cloud data centres.
- **Regular Audits**: Conducting regular audits of data processing activities and security measures.
- **Incident Response**: Establishing procedures to detect, report, and respond to data breaches.

8. Cloud Data Management

Given the use of cloud data centres, SCALA ensures:

- **Cloud Service Provider Selection**: Choosing cloud service providers with strong data protection policies and practices, ensuring compliance with PDPA, GDPR, and other relevant laws.
- **Data Encryption**: Ensuring that data stored in cloud environments is encrypted and access is controlled through robust authentication mechanisms.
- **Regular Assessments**: Conducting regular risk assessments and security audits of cloud service providers to ensure the ongoing protection of personal data.
- **Data Residency Requirements**: Complying with any data residency requirements stipulated by local laws and regulations.

9. Data Sharing and Transfers

SCALA will only share personal data with third parties when it is necessary and in compliance with applicable data protection laws. This includes:

- **Third-Party Agreements**: SCALA will enter into data processing agreements with all third parties who process personal data on our behalf, ensuring they provide adequate safeguards and comply with our data protection standards.
- **International Transfers**: Personal data transferred outside Singapore will only be transferred to countries that ensure an adequate level of data protection or under appropriate safeguards such as standard contractual clauses or binding corporate rules.

10. Data Retention and Disposal

SCALA will retain personal data only for as long as necessary to fulfill the purposes for which it was collected or to comply with legal, regulatory, or contractual requirements. Data that is no longer needed will be securely deleted or anonymized.

11. Data Breach Management

In the event of a data breach, SCALA will immediately contain the data breach. This is crucial to minimize damage and prevent further unauthorized access to data. Below are the key steps to take for immediate containment of a data breach:

11.1. Identify the Breach

- Detect the Breach: Use monitoring tools and systems to identify and confirm that a data breach has occurred. Look for unusual activity, alerts, or notifications from systems or personnel.
- Assess the Scope: Determine the nature and extent of the breach. Identify what data has been accessed, how it was breached, and which systems or networks are affected.

11.2. Isolate Affected Systems

- Disconnect Systems: If feasible, disconnect compromised systems from the network to prevent further unauthorized access. This might involve unplugging network cables, disabling wireless connections, or shutting down affected servers.
- Block Unauthorized Access: Use firewalls, network segmentation, and access controls to block further unauthorized access to systems or data.

11.3. Secure the Area

- Restrict Physical Access: Ensure that physical access to affected areas or systems is restricted to authorized personnel only.
- Preserve Evidence: Avoid making any changes to the affected systems until a proper assessment can be done. This helps preserve evidence for forensic analysis.

11.4. Activate the Incident Response Team

- Notify Key Personnel: Immediately inform the incident response team (IRT) or security team to take charge of the situation. This includes DPO, IT staff, security officers, and SCALA Management
- Implement Incident Response Plan: Follow the organization's predefined incident response plan to ensure a coordinated and effective response.

11.5. Implement IMMEDIATE Temporary Measures

- Change Passwords: Promptly change passwords for affected accounts and systems to prevent further unauthorized access.
- Revoke Access: Revoke access for users or systems identified as compromised or suspected of being involved in the breach.
- Deploy Patches and Updates: Inform IT Department to apply security patches or updates to systems that may have been exploited during the breach.

11. 6. Communicate Internally

- Inform Staff: Communicate the breach to relevant internal stakeholders, including IT, legal, management teams, Directors, to keep them informed of the situation and containment efforts.
- Maintain Confidentiality: Ensure information about the breach is shared on a need-to-know basis to prevent panic and protect sensitive details.

11.7. Document Actions Taken

- Record Events: Document all actions taken to identify, contain, and respond to the breach. This includes times, decisions, and personnel involved.
- Log Evidence: Maintain logs and records of affected systems, compromised data, and any forensic evidence collected during the containment process.

11.8. Monitor and Analyse

- Continuous Monitoring: Keep monitoring affected systems and networks for any signs of ongoing malicious activity or new threats.

- Perform Initial Analysis: Conduct a preliminary analysis to understand the breach's entry point, method, and scope, which will inform further actions.

11.9. Notify External Parties (if necessary)

- Regulatory Authorities: If required by law or regulation, notify relevant regulatory authorities within the mandated timeframe (e.g., the Personal Data Protection Commission (PDPC) in Singapore for significant breaches).
- Affected Individuals: Prepare to notify affected individuals if their data is at risk, including providing guidance on how they can protect themselves.

12. Employee Responsibilities

All employees of SCALA have a responsibility to ensure the protection and proper management of personal data. This includes:

- Training: Completing regular data protection training to stay informed about data protection policies and practices.
- Compliance: Adhering to the principles and procedures outlined in this policy.
- Reporting: Reporting any data breaches or security incidents immediately to the Data Protection Officer (DPO).

13. Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for overseeing SCALA's data protection strategy and implementation to ensure compliance with data protection laws. Unless otherwise appointed, the DPO shall be the Ops and Admin Manager.

The DPO's responsibilities include:

13.1. Monitor Compliance with Data Protection Laws

- Ensure Legal Compliance: Oversee the organization's compliance with relevant data protection laws and regulations, such as the GDPR, PDPA, and other applicable laws.
- Internal Audits: Conduct regular audits and assessments to ensure data processing activities comply with legal and organizational requirements.
- Data Protection Policies: Develop, implement, and maintain data protection policies and procedures within the organization.

13.2. Advise on Data Protection Impact Assessments (DPIAs)

- Evaluate Risks: Advise and assist with Data Protection Impact Assessments to evaluate the risks associated with data processing activities, particularly those involving sensitive data or high-risk operations.
- Mitigate Risks: Recommend measures to mitigate identified risks to data subjects' privacy and ensure compliance with data protection principles.

13.3. Raise Awareness and Provide Training

- Staff Training: Ensure that adequate data protection training and awareness programs for employees, contractors, and other relevant stakeholders are conducted
- Awareness Campaigns: Promote a culture of data protection and privacy awareness across the organization.

13.4. Serve as the Point of Contact for Data Subjects

- Respond to Inquiries: Act as the primary contact for data subjects regarding their rights, such as access requests, corrections, or objections to data processing.
- Complaint Resolution**: Address and manage data protection complaints and concerns raised by data subjects or employees.

13.5. Liaise with Supervisory Authorities

- Regulatory Communication: Serve as the point of contact for regulatory authorities on issues related to data protection, including reporting data breaches and compliance matters.
- Compliance Reports: Prepare and submit required reports and documentation to supervisory authorities as necessary.

13.6. Oversee Data Breach Response

- Incident Management: Coordinate the response to data breaches, including identification, containment, investigation, and remediation.
- Notification Obligations**: Ensure timely notification to regulatory authorities and affected individuals when required by law.

13.7. Advise on Data Processing Activities

- Data Handling Guidance: Provide guidance on data processing activities, including collection, use, storage, and sharing of personal data.
- Third-Party Assessments: Assess and advise on data protection risks associated with third-party vendors and service providers, if any.

13.8. Maintain Records of Processing Activities (RoPA)

- Document Processing Activities: Maintain comprehensive records of all personal data processing activities, including the purpose, scope, and legal basis for processing.
- Regular Updates: Ensure these records are regularly updated and accessible for review and compliance purposes.

13.9. Promote Data Protection by Design and Default

- Embed Privacy: Promote and implement the principles of data protection by design and by default in all projects, systems, and processes involving personal data.
- Project Involvement: Participate in the development and review of new projects, technologies, and business practices to ensure data protection considerations are

13.10. Develop and Implement Data Protection Strategies

- Strategic Planning: Develop and implement strategic plans to enhance data protection measures and compliance within the organization.

- Policy Development: Create and update data protection policies, procedures, and guidelines in line with evolving laws and best practices.

13.11. Facilitate and Oversee Data Transfers

- International Transfers: Ensure that data transfers, especially cross-border data flows, comply with applicable data protection regulations and use appropriate safeguards.

- Data Sharing Agreements: Review and manage data sharing agreements and contracts with third parties to ensure compliance with data protection standards.

13.12. Conduct Data Protection Audits

- Regular Audits: Perform or commission regular data protection audits to evaluate the effectiveness of data protection measures and identify areas for improvement.

- Audit Follow-up: Ensure that audit findings are addressed and that corrective actions are implemented in a timely manner.

13.13. Engage with Data Protection Community

- Stay Informed: Stay updated on the latest developments in data protection laws, technologies, and best practices through continuous learning and engagement with the data protection community within Supply Chain City (SCC)

- Networking: Build and maintain relationships with other DPOs, industry experts, and professional bodies to exchange knowledge and insights.

13.14. Prepare for and Respond to Data Subject Access Requests (DSARs)

- Manage Requests: Oversee the process for handling Data Subject Access Requests, ensuring they are processed within legal timeframes and in accordance with policy.

- Compliance Assurance: Ensure that responses to DSARs comply with all legal and regulatory requirements.

13.15. Advise on Data Protection Strategy and Governance

- Strategic Advisory: Advise the organization's leadership on data protection strategy, governance, and risk management.

- Governance Structures: Help establish and maintain governance structures for effective data protection management and oversight.

13.16. Risk Management and Incident Reporting

- Risk Assessments: Conduct regular risk assessments related to data protection and develop strategies to mitigate identified risks.

- Incident Reporting: Implement and manage a process for internal reporting of data protection incidents and issues.

14. Contact Information

For questions or concerns regarding this policy, please contact our Data Protection Officer at

Email: dpo@scala.com.sg

Phone: 87859665

Any query or complaint should include, at least, the following details:

- Your full name and contact information
- Brief description of your query or complaint

We treat such queries and feedback seriously and will deal with them confidentially and within reasonable time.