Serendib Financial Pty Ltd

Response to the AUSTRALIAN PRIVACY PRINCIPLES 2014

Part 1- Consideration of Personal Information Privacy

APP-1 Open and Transparent Management of Personal Information:

1.1 Serendib Financial Pty Ltd Financial Pty Ltd manages personal information openly and transparently.

1.2 Serendib Financial Pty Ltd takes steps as are reasonable in the circumstances to implement practices, procedures and systems relating to our function or activities that:

(a) Will ensure that we comply with the Australian Privacy Principles and these bind us; and

(b) This will enable us to address inquiries or complaints from individuals about our compliance with the Australian Privacy Principles.

1.3 Serendib Financial Pty Ltd has a clearly expressed and up-to-date policy about the management of personal information by us.

1.4 Our Response to Australian Privacy Principle 2014:

(a) Serendib Financial Pty Ltd collects the following information. It holds it for execution of transactions throughout the channel of distribution to fulfil our obligations imposed on by the Anti-Money Laundering and counter terrorism Act 2006 and its continuing amendments like the performance of transaction monitoring, due diligence and enhanced due diligence, record keeping and any other obligation imposed on us by any commonwealth legislation and or international treaties binding on us under territorial extension of the transactions.

Circumstance	Customer
KYC-Customer	Government-issued ID in proof of Full Name, Date of Birth, Address, Sample Signature, ID Sequence, Photo, Issue Date, expiration date, Occupation, Sex, Phone and Email Details. Purpose and Source of Transactions.
KYC-Institutions	A government-issued document that gives birth to the institution, Date of Incorporation, Office Address, ID Sequence, Issue Date, expiration date, Occupation, Phone and Email Details. Purpose and Source of Transactions. Information that links the Individuals legally representing the institution.
Due Diligence	We will screen by running the above details with DFAT, local and international sanctions lists, and adverse information domains for possible threats that may emerge from transacting with the customer.
Enhanced Due Diligence	When suspicion arises, we will seek more information to prove the purpose, source, and people involved in the transactions, including pay slips, bank statements, invoices, and/or agreements to prove the existence of legitimate relationships.
Instituted investigations	We will engage third-party experts to conduct enhanced due diligence about people we are involved in doing transactions with if they escalate as risk beyond tolerance.
Enforcement Actions	We will transfer your asset and pass on records in our custody to enforcement authorities in Australia and or authorities overseas under binding treaties if warranted and or issued with a subpoena.
Passing information to financial intelligence Units in Australia.	We will pass on all information about your transactions to AUSTRAC, the Australian Financial Intelligence Unit (FIU).

(b) We collect this information and hold it in electronic and hard formats in a secure manner.

(c) We collect this information because it is required for executing the transaction, and one or more commonwealth legislation obligates us to collect, analyze, report, and retain it to enforce certain governance frameworks.

(d) Our customers may access our branches in person during our working hours or contact us via email to request corrections to their records. Any changes must be supported by acceptable proof and will be processed in compliance with all relevant legislation governing our industry.

(e) Complaints about how we have addressed their request and or about our breach of APP to:
Mrs. Dammika Wijesekara, Compliance Officer,

We will take immediate action and endeavour to find a remedy as soon as practicable, with a maximum time limit of 30 days from receiving such complaints.

1.5 Serendib Financial Pty Ltd takes reasonable steps to make its response to Australian Privacy Principles available:

(a) Free of charge; and

(b) This is available for download in pdf format on our website; customers may ask for a hard copy printed and handed to them by approaching one of our branches in person.

1.6 If a person or body requests a copy of the APP Privacy Policy of Serendib Financial Pty Ltd in a particular format, we will take steps as reasonable in the circumstances to give the person or body a copy in that format.

APP-2 Anonymity and Pseudonymity:

2.1 Serendib Financial Pty Ltd does not allow individuals and bodies to remain anonymous or assume pseudonymity.

2.2 Privilege under 2.1 does not apply to customers of Serendib Financial Pty Ltd about this matter:

(a) The Anti-Money Laundering and Counter-Terrorism Act 2006 mandates us to identify, conduct due diligence, monitor transactional behaviors, report certain details when circumstances arise and retain their record for a statutory period. Therefore, we cannot deal with individuals who have not identified themselves; and

(b) It is impracticable for Serendib Financial Pty Ltd to deal with individuals who have not identified themselves or used pseudonyms.

Part 2- Collection of Personal Information

APP-3 – Collection of Solicited personal information

Personal Information Other than Sensitive Information

3.1 Serendib Financial Pty Ltd will collect personal information and record, retain, and analyze it; these are essential for the functioning of this business.

3.2 As an organisation, Serendib Financial Pty Ltd will collect personal information, which is essential for executing customer transactions.

Sensitive Information

3.3 Serendib Financial Pty Ltd does not collect sensitive information from its customers during the normal course of business. Therefore, clauses 3.3 and 3.4 are not applicable.

Means of Collection

3.5 Serendib Financial Pty Ltd collects personal information only by lawful and fair means.

3.6 Serendib Financial Pty Ltd collects personal information only from the individual and from information domains that authenticate this information provided by the individuals. We are required by AML CTF Law to do so while conducting due diligence and enhanced due diligence.

APP-4 Solicited Personal Information

4.1 If:

(a) We receive personal information; and

(b) We did not solicit the information; within a reasonable period after receiving it, we must determine whether we could have collected the information under APP3 if we had solicited it.

4.2 We may use or disclose personal information for the purpose of making the determination under subclause

4.3 If we determine that we have not collected personal information and the information is not contained in a Commonwealth record, we must, as soon as practicable but only if lawfully reasonable for us to do so, destroy the information or ensure that information is de-identified.

4.4 If sub clause 4.3 does not apply to personal information, APP 5 to 13 apply as if we had collected the information under APP-3.

APP-5 Notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, we collect personal information about an individual, we must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in sub-clause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of sub-clause 5.1 are as follows:

(a) the identity and contact details of us.

(b) If:

(i) We collect personal information from someone other than the individual; or

(ii) the individual may not know we have collected the personal information.

The fact that we collect, or collected, the information and the circumstances of that collection.

(c) if the collection of the personal information is required or authorized by or under an Australian Law or a court/tribunal order- the fact that the collection is so required or authorized (including the name of the Australian Law or details of the court/tribunal order, that requires or authorizes the collection);
(d) the purposes for which we collect the personal information.
(e) the main consequences (if any) for the individual if we do not collect all or some of the personal information.
(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which we usually disclose personal information of the kind collected by us;

(g) that the individual may access the personal information about the individual that we hold and seek correction of such information by presenting proof of such correction by presenting yourself to our office or writing to us with attested proofs of such correction to

The Chief Information Officer,

(h) the individual may complain about our breach of APP or a registered code that binds us to Australian Privacy Commissioner.

(i) We are likely to disclose information to overseas entities, but they are bound to observe the APP; we have taken reasonable steps to observe utmost care not to let them breach the APP.

(j) As we are likely to disclose personal information to our overseas partners in completing transactions, you may contact us to receive the details of overseas entities. Your information may have been passed on in writing to the Chief Information Officer,

Part 3- Dealing with Personal Information

APP-6 – Use or disclosure of personal information

Use or disclose

6.1 Our clients expressly consent to the collection and the way we must maintain this information under the legislative and regulatory framework in Australia.

6.2 We only disclose on occasion.

(a) the individual would reasonably expect the APP entity to use or disclose the information for a secondary purpose, and the secondary purpose is:

(i) if the information is sensitive information—directly related to the primary purpose; or

(ii) if the information is not sensitive information—related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(c) a permitted general situation exists about the use or disclosure of the information by the APP entity;

APP-6 – Use or disclosure of personal information.

6.1 Our clients expressly consent to the collection and the way we must maintain this information under the Australian legislative and regulatory framework.

6.2 We only give access to the enforcement agencies and or fulfil our obligations under Australia's AML/CTF Act.

APP-7 – Direct Marketing

7.1 We will not direct marketing with our clients using their personal information in our custody without their express consent.

7.2 We will not share their information with any third parties or with any of our associates in any case.

7.3 we will cease engaging in direct marketing with our clients from the time they ever ask us not to.

APP-8 Cross border Disclosure of Personal Information

We do not disclose personal information to any cross-border entities except as required to process international remittances. Transactions sent to the Bank of Ceylon (BOC) in Sri Lanka include necessary customer details as mandated by financial regulations and compliance requirements. All transfers are conducted securely and in accordance with Australian Privacy Laws, the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), and international remittance standards.

APP-9—adoption, use or disclosure of government-related identifiers.

We do not use any of the government-related identifiers that might be in our custody to index, store or retrieve any of our customer data.

Part 4- Integrity of personal information

APP-10 – Quality of personal information

10.1 We always endeavour to ensure that the information we gather about our clients is up to date by asking about their changing circumstances and when their Identity documents are up for renewal.

10.2 We also receive and update all the voluntary changed information about our clients submitted to us.

10.3 We make all reasonable efforts to ensure that the information we hold is updated, verified, and relevant to our conduct of business with our clients.

APP-11 Security of personal information

11.1 We are committed to and endeavour to keep our customer data secure from hacking, leakage, corruption, technological failure, and employee fraud.

Data Breach Response & Notification

Serendib Financial is committed to protecting the personal information of our customers. In the event of a data breach that is likely to result in serious harm, we will take immediate steps to contain the breach and assess the potential impact.

If a data breach occurs, we will:

1. **Assess the Breach** – Determine the nature and extent of the breach, including what personal information has been affected.
2. **Mitigate Risks** – Take all reasonable steps to contain the breach and prevent further unauthorized access.
3. **Notify Affected Individuals** – If we determine that the breach is likely to result in serious harm, we will notify affected customers as soon as possible, outlining:
    - The nature of the breach,
    - The types of personal information involved,
    - Recommended steps to mitigate potential harm.
4. **Report to Authorities** – If required, we will notify the **Office of the Australian Information Commissioner (OAIC)** and any relevant regulatory bodies in compliance with the **Notifiable Data Breaches (NDB) scheme**.

5. **Review & Prevent** – Investigate the cause of the breach and implement additional security measures to prevent future incidents.

For any data security concerns, customers can contact us at info@serendib.com.au.

11.2 We make periodical backups of our customers' transactional and profile data and store them in retrievable media for a minimum of seven years. However, this extends to a maximum of seven years from the date the customer ceases to deal with us.

Part 5- Access to and correction of personal information

APP-12 – Access to personal information

12.1 We commit to allowing access to the personal information of our clients we hold, at reasonable notice, in writing.

APP-13 Correction of personal information

13.1 We are committed to updating and correcting any inaccurate or outdated information we hold about our customers upon receiving valid proof.