Privacy Statement for Pillars Consultancy Limited

Introduction

At Pillars Consultancy Ltd ("**PC**"), we are dedicated to protecting the privacy and personal information of our clients, and partners. This Privacy Statement outlines how we collect, use, disclose, and protect personal information in accordance with Bermuda's Personal Information Protection Act 2016 ("**PIPA**").

1. Collection of Personal Information

We collect personal information necessary for the effective operation of our business and to provide high-quality advisory and compliance services. This includes:

Contact details (name, address, phone number, email address)

Employment details (job title, department, employment history)

Compliance-related information (client's business practices, company corporate information, regulatory requirements, and compliance statuses)

2. Use of Personal Information

The personal information we collect is used for various purposes, including:

Contact Information: Names, addresses, phone numbers, and email addresses of clients.	1. **Communication**: To maintain effective communication with clients regarding compliance matters, updates, and regulatory changes.

	2. **Service Delivery**: To provide personalized services and support tailored to the specific needs of each client. 3. **Legal and Regulatory Requirements**: To comply with legal obligations, such as verifying client identities and maintaining accurate records for audits and inspections. 4. **Consent and Preferences**: To manage and respect our clients' preferences and consents regarding the use of their personal information These practices ensure that we can operate efficiently while adhering to PIPA's principles of lawful, fair, and secure information & data handling.
Identification Data: National identification numbers, passport details, and other government-issued identification.	1. **Verification and Authentication**: To verify the identity of clients and ensure that they are who they claim to be. This is crucial for preventing fraud and ensuring the integrity of the advisory services. 2. **Regulatory Compliance**: To comply with legal and regulatory requirements, such as anti-money laundering (AML) and know-your-customer (KYC) regulations, which mandate the collection and verification of identification data. 3. **Record Keeping**: To maintain accurate and comprehensive records for audits, inspections, and potential legal inquiries. This helps in demonstrating compliance with various laws and regulations. 4. **Risk Management**: To assess and manage risks associated with providing advisory services, including identifying potential conflicts of interest and ensuring

	that services are provided to legitimate clients These practices help ensure that we operate within the legal framework and maintain high standards of security and trust.
Financial Information: Bank account details, transaction histories, and financial statements.	1. **Regulatory Compliance**: To comply with anti-money laundering (AML) and know-your-customer (KYC) regulations, which require detailed financial information to verify the legitimacy of clients' financial activities. 2. **Risk Assessment**: To assess and manage financial risks associated with their clients, ensuring that they are not involved in fraudulent or illegal activities. 3. **Service Provision**: To provide accurate and tailored compliance services based on a comprehensive understanding of the client's financial situation. 4. **Audit and Reporting**: To maintain accurate records for audits, inspections, and regulatory reporting, demonstrating compliance with financial regulations These practices help ensure that we operate within the legal framework and maintain high standards of security and trust.
Employment Records: Job titles, employment history, training, and performance evaluations.	1. **Client Verification**: To verify the identity and credibility of clients, ensuring they are legitimate and trustworthy. 2. **Risk Assessment**: To assess the financial and operational risks associated with clients, particularly in industries where employment history and performance can impact compliance and regulatory risks.

	3. **Service Customization**: To tailor compliance advice and services based on the specific needs and backgrounds of clients, ensuring more effective and relevant support. 4. **Regulatory Compliance**: To meet legal and regulatory requirements that may necessitate detailed records of clients' professional backgrounds These practices help ensure that we can provide accurate, compliant, and effective advisory services while adhering to PIPA's principles of lawful and secure data handling.
Sensitive Personal Information: Health information, biometric data, and any other sensitive information necessary for compliance purposes.	1. **Regulatory Compliance**: To comply with specific legal and regulatory requirements that mandate the collection of sensitive data for certain clients or transactions. This is often necessary for industries with stringent compliance standards. 2. **Risk Management**: To assess and manage risks associated with providing advisory services, particularly in cases where sensitive information is crucial for understanding the full scope of a client's situation. 3. **Service Customization**: To provide tailored advice and services that take into account the unique needs and circumstances of our clients, especially when sensitive information is relevant to the advisory process. 4. **Security and Authentication**: To enhance security measures, such as using biometric data for secure access to sensitive information or systems

	These practices help ensure that we can provide accurate, compliant, and effective advisory services while adhering to PIPA's principles of lawful and secure data handling.
Website & Social Media	If you use the website or comment feature on an online platform, or if you communicate with us through any of our social media (e.g. LinkedIn & website), you should be aware that any personal information you submit through comments or posts to the website or other social media forum can be read, collected, or otherwise used by anyone with access to the forum or who visits the URL of the web page on which the post or comment is posted.

3. Disclosure of Personal Information

We may disclose personal information to third parties for the following purposes:

- To service providers who assist us in delivering our advisory services and conducting our business operations
- For legal purposes, or regulatory authorities as required
- With the consent of the individual to whom the information pertains

4. Protection of Personal Information

We take reasonable steps to protect personal information from loss, unauthorized access, use, modification, or disclosure. These steps include:

- We implement appropriate technical and organizational measures to protect personal information from unauthorized access, disclosure, alteration, or destruction. These measures include:
- Secure storage systems.
- Access controls and authorization protocols.
- Regular data security assessments.
- Using technological safeguards such as secure access protocols

- Ensuring our staff are trained in the handling of personal information in accordance with PIPA
- Where we use service providers who might have access to your personal information, we select them carefully and require them to have privacy and security standards that are comparable to ours. We use contracts and other measures with our service providers to ensure that they maintain the confidentiality and security of your personal information and to prevent such information from being used for any other purpose, in accordance with PIPA.

5. Rights of Individuals

Individuals have the right to:

- Access their personal information
- Request corrections to their personal information
- Withdraw consent for the collection, use, or disclosure of their personal information, subject to legal and contractual restrictions

8. Compliance-Related Information

We collect and use compliance-related information to provide our advisory services effectively. This includes assessing our clients' business practices, regulatory requirements, and compliance statuses. We handle this information with the utmost confidentiality and security.

9. Contact Us

If you have any questions or concerns about our privacy practices, or if you wish to exercise your rights, please contact us at:

Pillars Consultancy Limited

16 Burnaby Street, Hamilton

Bermuda

Email: Michelle@pillars.bm

You may also enquire about how your personal information should be handled, or accessed, with the office of the Privacy Commissioner by contacting Privcom@privacy.bm with any concerns.

10. Conclusion

We are committed to protecting the privacy of all individuals whose personal information we hold or collect. We continuously review and update our privacy practices to ensure compliance with Bermuda's Personal Information Protection Act 2016 (PIPA).

Date: 1 January 2025