— PRIVACY POLICY DOCUMENT —

VG FINANCIAL SERVICE

Privacy Policy

Personal Information Protection

Established under Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA)
and British Columbia's *Personal Information Protection Act* (PIPA)
Applicable to the Company and all clients

Policy Version	v1.0
Effective Date	January 2026
Next Review	January 2027
Issued By	VG Compliance Committee

V G

SINCE 2013 · FINTRAC REGISTERED MSB

VOL.1

CONFIDENTIAL

— TABLE OF CONTENTS —

Contents

SECTION 01

Our Privacy Commitment

VG Financial (Vangead International Enterprises Ltd., hereinafter "the Company") recognizes the sensitivity of client personal and financial information. As a FINTRAC-registered Money Services Business in Canada, the Company simultaneously fulfils its anti-money-laundering obligations and **upholds client privacy protection as a core commitment**.

This Policy is established under:

- **PIPEDA** — Canada's federal *Personal Information Protection and Electronic Documents Act*
- **BC PIPA** — British Columbia's *Personal Information Protection Act*
- **PCMLTFA** — Canada's *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (which imposes compliance-data retention requirements)

Three Core Commitments

① We **do not sell, rent, or exchange client data** with any advertiser or marketing company.
② Inquiries that do not result in a transaction are **deleted immediately upon confirming no further interest**.
③ Client data is shared with third parties **only where legally required or operationally necessary**.

Each transaction, inquiry submission, or visit to the Company's website constitutes acceptance of the version of this Policy then in effect. If a client does not agree with any term, the client should not submit personal information.

SECTION 02

Personal Information We Collect

The scope of information collected varies by stage of engagement, following the **"minimum necessary" principle**:

① Website Inquiry Stage (Prospective Clients)

Basic contact information	Name, phone number, email
Inquiry details	Service type, anticipated amount, free-text notes
Website analytics	IP address, browser type, pages viewed (see SECTION 05)

② KYC Onboarding Stage (Confirmed Clients)

As required by FINTRAC and the PCMLTFA, the Company must collect the following before any transaction:

Government ID	Passport, driver's licence, or Canadian permanent-resident card (copy or scan)
Proof of address	Bank statement, utility bill, or government correspondence dated within the last 3 months
Source of funds	Pay statements, tax returns, investment-income records, or similar (mandatory for amounts ⩾ CAD 10,000)
Bank account details	Bank name, account number, and SWIFT code for the sending and receiving accounts
Corporate clients (additional)	Certificate of incorporation, Beneficial Owner information, and authorized-signatory documentation

③ Communications & Service Stage

Messaging handles	WeChat ID, WhatsApp number (recorded only when voluntarily provided by the client)
Communication records	Call recordings and summarized message exchanges between client manager and client (where applicable)
Service preferences	Frequently used banks, currencies, and purposes mentioned by the client

④ Transaction Execution Stage

Transaction records	Amount, timestamp, currency, counterparty, SWIFT MT103 messages
Contract documentation	Service agreement, risk-disclosure form, and signature records

> **On sensitive information:** The Company does not actively collect sensitive information unrelated to its services (such as health records, religious beliefs, political views, or sexual orientation). Where a client volunteers such information, it is treated as non-essential and is not included in the KYC file.

⑤ How We Collect Information

- Information voluntarily submitted by the client (website forms, email, paper documents)
- Documents presented in person at a branch and scanned for our records
- Notes taken by the client manager during communications
- Third-party compliance databases (used solely for PEP and sanctions-list screening)

SECTION 03

How We Use Information

The Company uses client information solely for the following purposes:

Core Service Purposes

- **Onboarding & KYC verification**: confirming client identity in accordance with FINTRAC requirements
- **Inquiry response**: providing quotes, walkthroughs, and client-manager introductions
- **Transaction execution**: initiating cross-border wires and foreign-exchange settlements via the SWIFT network
- **Client service**: enquiries and post-transaction support by phone, WhatsApp, or in-branch
- **Funds tracing**: assisting clients to track wire status and resolve credit anomalies

Compliance & Legal Purposes

- FINTRAC statutory reporting (LCTR, STR, TPR, EFT)
- Anti-money-laundering and counter-terrorist-financing risk assessment
- Sanctions-list and PEP screening
- Responding to regulatory audits, judicial investigations, and tax reviews

What We Will Not Use Information For

The Company **will not use client information for any of the following**:

- Sale or rental to third-party advertisers or marketing companies
- Retargeting advertising
- Third-party data exchange or co-marketing referrals
- Commercial promotion of products or services unrelated to VG's business

SECTION 04

Sharing with Third Parties

The Company shares client information with third parties **only in the following two circumstances**:

① Statutory Regulatory Requirements

Pursuant to the PCMLTFA and related law, the Company is required to provide client and transaction information to the following:

- **FINTRAC** — the Financial Transactions and Reports Analysis Centre (LCTR, STR, EFT reports)
- **RCMP** — the Royal Canadian Mounted Police (Terrorist Property Reports and criminal-investigation cooperation)
- **CRA / Service Canada** — the Canada Revenue Agency or other government bodies (pursuant to a lawful production order)
- **Courts / arbitral bodies** — pursuant to lawful production orders, subpoenas, or judgments

② Operational Necessity

To execute a client's remittance or exchange instructions, the Company must share necessary information with:

- **SWIFT network** — the international interbank messaging system used for cross-border wires
- **Partner banks** — the receiving and remitting banks designated by the client (in Canada, China, Hong Kong, and elsewhere)
- **Settlement & clearing institutions** — offshore RMB (CNH) clearing houses and settlement banks

The information shared is strictly limited to fields required to execute the transaction (payer/payee name, account number, amount, currency, purpose code, etc.), and **excludes the client's non-transactional personal information**.

> **Explicit statement:** The Company does not share client information with advertising platforms, marketing-service providers, data-analytics firms, business partners, insurers, real-estate agencies, or any other commercial third party.

SECTION 05

Website Analytics

The Company's website (www.vangead.com) uses **Google Analytics** for basic visitor statistics, with the goal of understanding usage and improving the user experience.

What Google Analytics Collects

- Visitor IP address (automatically anonymized)
- Device type, browser, and operating system
- Page paths visited and time spent on each page
- Traffic source (search engine, direct visit, or external link)
- Approximate geographic location (city level)

Google Analytics data is processed and stored by Google and is subject to Google's own privacy policy. See:
policies.google.com/privacy

Tracking Technologies We Do Not Use

The Company **does not use** any of the following:

- Social-media tracking pixels such as Facebook / Meta Pixel
- Chinese-market tracking tools such as Baidu Tongji or TikTok Pixel
- Cross-site retargeting advertising cookies
- Third-party marketing-automation platforms (HubSpot, Salesforce Pardot, etc.)
- Session-recording tools (Hotjar, FullStory, etc.)

How to Opt Out

Visitors can opt out of Google Analytics tracking by any of the following:

- Installing the official **Google Analytics Opt-out Browser Add-on**
- Enabling "Do Not Track" in browser settings
- Visiting the site in private / incognito browsing mode

SECTION 06

Data Storage & Cross-Border Transfer

Primary Storage Locations

Client data is primarily stored **within Canada**. However, given the architectural realities of modern financial services, some data may be stored in or pass through the following:

- **Canada (primary)** — Company servers and Canadian-domiciled cloud services
- **U.S. cloud services** — North American cloud platforms such as Google Workspace and Microsoft 365 (email and document collaboration)
- **Hong Kong / offshore settlement nodes** — used solely on the necessary clearing path for cross-border remittance
- **SWIFT network** — international interbank messaging nodes (headquartered in Belgium with global distribution)

> **On cross-border transfer:** When information moves across jurisdictions, the Company ensures that the receiving jurisdiction provides privacy protection **at least equivalent to Canada's PIPEDA standard**, or executes a data-processing agreement (DPA) under Canadian law with the recipient.

Chinese Messaging Handles Provided by Clients

Where a client voluntarily provides a WeChat ID, WhatsApp number, or similar handle for communication, related messages may reside on that platform's servers and are subject to that platform's privacy policy. We recommend that clients **use email or in-branch delivery** for sensitive material (government IDs, bank-account details) rather than instant-messaging tools.

Visitors from Mainland China

Data collection from mainland-China visitors follows this Policy in full. Where Google Analytics fails to load — as can occur in parts of mainland China — no analytics data is collected.

SECTION 07

Data Retention Periods

Retention periods vary by data type as follows:

Inquiries that did not transact	Where an inquiry is submitted but the client does not proceed to onboard, the records are **deleted immediately upon confirming no further interest**. The Company does not retain such contact information for subsequent marketing.
Website analytics	Google Analytics retains data for 14 months by default; automatic deletion thereafter.
KYC compliance file	Client identification documents, source-of-funds declarations, and similar records are **retained for at least 5 years** from the date of the last transaction (PCMLTFA statutory requirement).
Transaction records	Amounts, counterparties, timestamps, and other transaction details are **retained for at least 5 years** from the date of completion (PCMLTFA statutory requirement).
Regulatory-report copies	LCTR / STR / TPR / EFT reports and related supporting materials are **retained for at least 5 years**.
Communication records	Phone, email, and instant-messaging records are retained for 5 years alongside the corresponding transaction file. Communications associated with non-transacting inquiries are deleted together with the inquiry.

> **On "immediate deletion":** The Company's policy of immediately deleting non-transacting inquiries is **at the stricter end of industry practice**. Many financial-service providers retain leads for years for remarketing; the Company has chosen immediate deletion to maximize client privacy.

Disposal After Retention Period

Electronic files past the retention period are destroyed by **non-recoverable means** (overwrite-based erasure); paper files are destroyed by **professional shredding services**. Destruction logs are retained for 1 year for audit purposes.

SECTION 08

Data Security Safeguards

Technical Safeguards

- **Encryption in transit** — TLS 1.2+ for all website forms, email, and the client-management system
- **Encryption at rest** — AES-256 for database storage
- **Access control** — least-privilege authorization; employees can access only the client data required for their duties
- **Two-factor authentication** — 2FA mandatory for all internal-system logins
- **Regular backups** — daily off-site backups of critical data; backup media are likewise encrypted

Administrative Safeguards

- All employees sign confidentiality agreements; obligations continue for 5 years post-departure
- Regular privacy and compliance training
- Documented privacy-incident response procedure (see below)
- At least one third-party security audit per year

Physical Safeguards

- Branches are equipped with safes and surveillance systems
- Paper files are kept in locked cabinets accessible only to authorized personnel
- Access control on office areas

Privacy-Incident Response

In the event of a data breach or suspected breach, the Company will:

- Immediately initiate containment and damage-mitigation measures
- Assess scope of impact within 72 hours
- **Proactively notify affected clients in writing**
- Report to the Office of the Privacy Commissioner of Canada (OPC) as required by PIPEDA
- Provide remedies such as identity-theft monitoring where warranted

SECTION 09

Client Rights

Under PIPEDA and BC PIPA, clients have the following rights regarding personal information held by the Company:

① Right to Know

Clients have the right to know what information has been collected, for what purposes, and with whom it is shared. This Policy serves as the consolidated disclosure.

② Right of Access

Clients may submit a written request to the Privacy Officer to **access the personal information the Company holds about them**. The Company will respond within 30 days.

③ Right to Correction

Where information held is inaccurate or incomplete, clients may request correction. After verification, the Company will promptly amend the record.

④ Right to Withdraw Consent

Clients may withdraw consent at any time. **However, please note:**

- Withdrawal of consent may prevent the Company from continuing to provide services to the client
- Records of completed transactions **must still be retained for 5 years** under the PCMLTFA and cannot be immediately deleted
- Compliance reports already filed with FINTRAC cannot be retracted

⑤ Right to Erasure (limited by law)

Clients may request immediate deletion of information not subject to a statutory retention requirement (such as non-transacting inquiries or expired analytics data). Data subject to the 5-year PCMLTFA retention obligation must be kept until that period expires.

⑥ Right to Complain

If a client believes the Company's privacy practices are non-compliant, the client may:

- First lodge a complaint with the Company's Privacy Officer (contact details on the next page)
- If the response is not satisfactory, escalate to the **Office of the Privacy Commissioner of Canada**

SECTION 10

Contact the Privacy Officer

For any question regarding this Policy, the handling of personal information, or the exercise of rights, the client may contact the Company's Privacy Officer:

- **Written correspondence**: send to any of the Company's branches, marked "Attention: Privacy Officer"
- **Official website**: www.vangead.com

The Company will provide an initial response **within 5 business days** of receipt and a complete response **within 30 days**.

External Complaint Channels

- **Office of the Privacy Commissioner of Canada (OPC)** — priv.gc.ca
- **Office of the Information and Privacy Commissioner for BC (OIPC BC)** — oipc.bc.ca

About This Policy

This Policy is established and issued by the Company's Compliance Committee and is reviewed and updated at least annually. Material legal or operational changes may trigger immediate revision. Amendments will be published on the Company's website and at its branches, taking effect from the date of publication. A client's continued use of the Company's services constitutes acceptance of the revised policy.

VG Compliance Committee

Vangead International Enterprises Ltd.
FINTRAC Registered MSB • M22975430
Greater Vancouver • 6 Branches
www.vangead.com