FCB NA LTD — Privacy Policy (Business Services)

Key Facts Summary

- **Scope.** This Policy explains how we handle personal information in connection with our **business payment services** for **corporate clients** (no consumer accounts).
- **Our role.** We act primarily as a **data controller** under **PIPEDA**; for certain integrations or bespoke processing we may act as a **data processor** under your instructions.
- **What we collect.** Identity/KYB/KYC data, contact details, role/permission info, due-diligence results (PEP/sanctions/adverse media), account/transaction metadata, technical security logs.
- **Why we use it.** To onboard your organization, provide and secure the services, meet legal and AML/CTF obligations, detect and prevent fraud/abuse, support you, bill you, and improve our services (often in aggregated or de-identified form).
- **Legal bases.** Contract performance, legal obligations, **legitimate interests**, and consents where required (e.g., some biometrics or marketing).
- **Sharing.** With regulated verification/screening vendors, cloud and security providers, correspondent banks and payment schemes, and competent authorities where lawful.
- **Transfers.** Data may be processed/transferred outside your province/country; we apply appropriate safeguards.
- **Retention.** We keep records as long as needed for the service and to meet legal/AML requirements (commonly **5–7 years** after relationship end).
- **Your rights.** Access, correction, deletion (where applicable), restriction/objection, portability (EU/UK), and complaint routes.
- **Security.** We use administrative, technical, and physical safeguards (encryption, MFA, access controls, logging).
- **Contact.** info@fcb.tm for privacy requests; you may also contact the relevant privacy regulator in your region.

This summary is for convenience only. The clauses below are legally binding.

---

1. Who We Are and What This Policy Covers

1.1 This Privacy Policy describes how FCB collects, uses, discloses, and protects **personal information** related to your organization's use of our business payment services, account portal, mobile/app, and APIs.
1.2 This Policy applies to personal information about **directors, officers, Authorized Persons, employees/contractors, beneficial owners/PSCs**, and other individuals whose

data you provide to us. It does **not** cover information that cannot reasonably identify an individual (e.g., anonymized/aggregated data).
1.3 Our services are for **corporate clients** only and are **not** directed to consumers or children.

---

2. What Personal Information We Collect

2.1 Identification & due-diligence

- Names, aliases, date/place of birth, nationality, government ID details, verification artefacts (e.g., selfie/biometric checks where permitted by law), beneficial ownership, PEP/sanctions/adverse-media results, source-of-funds/wealth information.

2.2 Business & contact details

- Employer/organization, job title/role, business email and phone, business addresses, authority/mandate status, approval thresholds.

2.3 Account & transaction data

- Account identifiers, beneficiaries and counterparties (business contact data), corridors and currencies used, payment metadata (amounts, timestamps, references), FX and fee metadata.

2.4 Technical & security logs

- Login and session telemetry, device/browser and IP data, MFA events, API key metadata, audit trail of approvals and changes, fraud signals.

2.5 Communications

- Support tickets, call/chat/email records, preferences, complaints, and feedback.

2.6 Sources

- You and your representatives; public/commercial registers; verification/screening providers; payment networks and correspondent institutions; fraud-prevention services; and, where lawful, competent authorities.

---

3. How We Use Personal Information (Purposes)

3.1 Service delivery & account administration

- Onboarding (KYB/KYC), enabling and operating the account portal/APIs, processing payments/FX, managing beneficiaries/permissions, customer support, billing.

3.2 Safety, security & fraud/AML

- Identity verification, sanctions/PEP/adverse-media screening, transaction monitoring, anomaly detection, incident response, business continuity and disaster recovery.

3.3 Legal and regulatory compliance

- Meeting AML/CTF, sanctions, tax and financial-services laws; responding to lawful requests from authorities; maintaining audit logs and records.

3.4 Service improvement & analytics

- Improving features, reliability, and user experience; measuring performance; creating **aggregated or anonymized** insights that do not identify individuals.

3.5 Business operations

- Vendor management, reporting, defending legal claims, financing or corporate transactions under confidentiality.

3.6 Communications & B2B marketing

- Operational and security notices; service updates. Limited **business-to-business** marketing relevant to our services, with opt-out at any time.

---

4. Legal Bases for Processing

4.1 Performance of a contract with your organization and steps taken at your request.
4.2 Legal obligations, including AML/CTF, sanctions, financial-services, bookkeeping and tax requirements.
4.3 Legitimate interests, such as operating secure services, preventing fraud/abuse, improving tools, and defending legal rights; we balance these interests against privacy rights.
4.4 Consent where required by law (e.g., certain biometrics or specific marketing). Consent may be withdrawn at any time; prior processing remains lawful.

---

5. Sharing and Disclosure

5.1 Service providers

- Identity verification, sanctions/PEP/adverse-media screening, fraud prevention, cloud hosting, security operations, communications, analytics (on de-identified data), and professional advisers—all under appropriate contracts and safeguards.

5.2 Financial ecosystem

- Correspondent banks, payment schemes, clearing systems, card/program partners, and other institutions as needed to execute transactions and comply with their rules.

5.3 Authorities and legal requests

- Competent authorities, courts, regulators, or law-enforcement where required or permitted by law, or to protect rights, safety, and security.

5.4 Corporate transactions

- Potential investors or acquirers under confidentiality, solely for evaluating or completing a financing, merger, acquisition, or reorganization.

---

6. International Data Transfers

6.1 Personal information may be **transferred** to, stored in, or accessed from countries other than yours.
6.2 Where required, we implement safeguards such as contractual clauses and risk assessments, and apply technical/organizational measures to help ensure a level of protection not materially less protective than in the originating jurisdiction.

---

7. Retention

7.1 We retain personal information as long as necessary to provide the services, meet legal/regulatory requirements (including AML/CTF record-keeping), resolve disputes, and enforce rights.
7.2 Retention periods commonly extend **5–7 years** after the end of the relationship or final transaction, subject to longer statutory retention in specific cases. Data is securely deleted or archived when no longer required.

---

8. Security

8.1 We employ administrative, technical, and physical safeguards appropriate to the sensitivity of the information, including access controls, MFA, encryption in transit and at rest where appropriate, network segmentation, vulnerability management, logging and monitoring, and staff training.
8.2 No system is perfectly secure. We maintain incident response processes and will notify authorities and affected individuals **where required by law**.

---

9. Your Choices and Rights

9.1 Access and correction (Canada & most regions)

- Request access to personal information we hold about you and ask for corrections of inaccuracies.

9.2 Deletion and restriction

- In some regions, request deletion, restriction, or objection to certain processing, subject to legal exceptions (e.g., AML/CTF retention).

9.3 Portability (EU/UK)

- In certain cases, receive data you provided in a portable format and request we transmit it to another controller where technically feasible.

9.4 Automated decisions

- Request human review of decisions that are solely automated and produce legal or similarly significant effects, where provided for by law.

9.5 Marketing

- Opt out of **B2B marketing** at any time via the link in messages or by contacting **info@fcb.tm**. Operational and security notices are not marketing and generally cannot be opted out of.

9.6 Exercising rights

- Send requests to **info@fcb.tm**. We may need to verify identity and scope. Some rights may be limited where access would prejudice investigations, breach confidentiality, or conflict with legal obligations.

---

10. Cookies and Similar Technologies

10.1 We use cookies and similar technologies to operate the portal, enhance security (including session management and fraud prevention), and understand aggregate usage.
10.2 Where required, we seek consent for non-essential cookies and provide controls to adjust preferences. Disabling certain cookies may affect functionality.
10.3 See our **Cookie Policy** for details on categories, purposes, and retention.

---

11. Children

11.1 Our services are intended for organizations and are **not** directed to children.
11.2 We do not knowingly collect personal information from individuals under the age permitted by applicable law for these purposes.

---

12. Automated Decision-Making and Profiling

12.1 We use automated systems to help verify identity, screen against sanctions/PEP/adverse-media, and detect fraud/AML risk.
12.2 These systems may generate risk scores and flags for **human review**; where local law grants specific rights, individuals may request an explanation of the decision logic and human intervention.

---

13. Changes to This Policy

13.1 We may update this Policy to reflect legal, technical, or business changes.
13.2 We will post updates with a new **effective date** and, where changes are material, provide reasonable notice.

---

14. How to Contact Us and How to Complain

14.1 Contact FCB (privacy): info@fcb.tm; or write to: Privacy Team, FCB NA LTD, 7030 Woodbine Ave, Suite 500, Markham, Ontario L3R 6G2, Canada.
14.2 Complaints (Canada): You may contact the **Office of the Privacy Commissioner of**

Canada (OPC) or, where applicable, the relevant provincial privacy commissioner.
14.3 Complaints (EU/UK): You may contact your local **supervisory authority** (EU) or the **UK Information Commissioner's Office (ICO)**. We encourage you to contact us first so we can try to resolve your concern.

---

15. Definitions

"Authorized Person": An individual your organization authorizes to access and operate the account.
"Personal information" / "personal data": Information about an identifiable individual.
"Processing": Any operation performed on personal information (collection, use, disclosure, storage, etc.).
"Pseudonymized": Processed such that the data cannot be attributed to a specific individual without additional information kept separately.
"Anonymized/Aggregated": Data altered so individuals are not identifiable.