Agility Forex U.S. Privacy Policy

This U.S. Privacy Policy explains how Agility Forex Ltd. (“Agility,” “we,” “us,” or “our”) collects, uses, discloses, retains, and protects personal information in connection with our U.S. services. It also describes the privacy rights and choices that may be available to you.

1. Scope and Relationship to Other Notices

This Policy applies to individuals who apply for, access, or use Agility’s U.S. foreign-exchange, payment, account, website, platform, customer-support, and related services. It also applies to beneficial owners, control persons, directors, officers, employees, authorized users, payers, payees, beneficiaries, and other individuals whose information is provided to us in connection with a business customer.

Agility is a Canadian money-services business and a foreign-exchange and payment-services provider registered with the U.S. Financial Crimes Enforcement Network as a money services business. Agility is not a bank. Certain U.S. deposit accounts and regulated banking services are provided by an applicable sponsor bank through program and technology partners.

Additional privacy notices or disclosures may apply depending on the services you use, your state of residence, and the financial institutions or service providers involved. These may include separate notices provided by an applicable sponsor bank, identity-verification provider, account-linking provider, or other financial institution. Each supplemental notice governs that party’s own practices or the specific service it covers and should be read together with this Policy. This Policy describes Agility’s practices and does not replace any legally required financial privacy notice or other disclosure.
This Policy does not apply to Agility employees or job applicants, or to third-party websites and services that have their own privacy notices.

2. Personal Information We Collect

The information we collect depends on the services you request, the capacity in which you interact with us, and applicable legal, regulatory, bank, network, and risk requirements.

2.1 Identity and Contact Information

We may collect your full legal name, aliases, date of birth, citizenship, residency, residential and mailing addresses, email address, telephone number, occupation, job title, and employer or business affiliation.

2.2 Government and Identity-Verification Information

We may collect Social Security numbers, Individual Taxpayer Identification Numbers, employer identification numbers, passport numbers, driver's license or state identification numbers, other government identifiers, issuing jurisdiction, document images, document expiry dates, photographs, selfies, liveness results, and identity-verification results.

Our identity-verification providers may collect photographs or selfies and use facial-comparison, liveness, or similar technology to verify identity and prevent fraud. Those providers may process biometric identifiers or biometric information under their own privacy notices. Agility generally receives the verification result and related risk signals rather than an underlying biometric template. Where Agility collects or possesses biometric information, it is used only for identity verification, fraud prevention, security, and legal compliance, and we provide any separate notice or consent and apply the retention and destruction requirements required by applicable law.

2.3 Business and Ownership Information

For business customers, we may collect legal and trade names, entity type, formation jurisdiction and date, registration and tax numbers, business addresses, websites, industry, products and services, licenses, organizational documents, ownership percentages, control information, and information about beneficial owners, control persons, directors, officers, authorized users, and other representatives.

2.4 Financial and Transaction Information

We may collect bank-account and routing information, account ownership information, funding instructions, balances made available through the services, transaction amounts, currencies, exchange rates, beneficiaries, counterparties, payment purposes, invoices, source-of-funds and source-of-wealth information, expected and actual activity, transaction history, fees, returns, disputes, and related records.

We do not request that you provide online-banking passwords directly to Agility. If you choose an account-linking service, your credentials are handled by that provider under its own privacy and security terms, and Agility generally receives account and verification data rather than your credentials.

2.5 Compliance, Fraud, and Risk Information

We may collect or generate customer-due-diligence records, sanctions and watchlist screening results, politically exposed person and adverse-media results, fraud indicators, device and behavioral risk signals, account and transaction alerts, investigations, case notes, risk ratings, and information obtained from regulators, law enforcement, courts, public records, and compliance-data providers.

2.6 Device, Website, and Usage Information

We may collect IP address, device identifiers, browser and operating-system information, login activity, timestamps, approximate location derived from IP address, referring and exit pages, pages viewed, clicks, session information, cookie identifiers, error logs, and security events.

2.7 Communications and Service Records

We may collect emails, messages, documents, support requests, complaints, instructions, preferences, and records of communications with you. We may record telephone or video calls for quality, training, security, dispute resolution, and compliance purposes where permitted by law and after providing any notice or obtaining any consent required by law.

2.8 Inferences and Derived Information

We may derive information from the data described above, such as account eligibility, fraud likelihood, transaction risk, anticipated service needs, and whether activity is consistent with your stated profile. We use automated tools to assist these reviews, but human review is available where required by law or appropriate to the decision.

3. Sources of Personal Information

We may obtain personal information directly from you; from a business customer or authorized representative; from beneficial owners, control persons, payers, payees, beneficiaries, and transaction counterparties; from sponsor banks, program managers, correspondent banks, payment networks, and other financial institutions; from identity-verification, bank-account-verification, fraud-prevention, sanctions, adverse-media, credit-reference, and compliance-data providers; from government agencies, regulators, law enforcement, courts, and public records; from service providers and professional advisers; and automatically from your device and use of our website or platform.

If you provide personal information about another individual, you represent that you are authorized to provide it and that any notice or consent required by law has been obtained.

4. How We Use Personal Information

We may use personal information to:

4.1 Provide and Administer Services

Open, verify, maintain, service, and close accounts; execute foreign-exchange and payment transactions; process funding, collections, settlements, returns, refunds, and fees; provide statements, confirmations, notices, disclosures, and support; and communicate with you about the services.

4.2 Verify Identity and Eligibility

Verify individuals and businesses; confirm account ownership and authority; assess eligibility; satisfy customer-identification, customer-due-diligence, beneficial-ownership, sponsor-bank, and payment-network requirements; and keep records current.

4.3 Prevent Fraud and Protect the Services

Authenticate users; detect, investigate, prevent, and respond to fraud, identity theft, account takeover, unauthorized activity, cybersecurity events, misuse, and other threats; protect customers, Agility, sponsor banks, service providers, and the public; and enforce contractual and platform controls.

4.4 Comply With Law and Manage Risk

Comply with anti-money-laundering, counter-terrorist-financing, sanctions, tax, recordkeeping, reporting, legal-process, regulatory, bank, network, and other obligations; conduct monitoring and investigations; respond to lawful requests; establish, exercise, or defend legal claims; and manage financial, operational, compliance, and reputational risk.

4.5 Improve and Operate Our Business

Maintain and improve our website, platform, products, service quality, workflows, models, security, and customer experience; conduct testing, analytics, audits, forecasting, and internal reporting; train personnel; manage vendors; and support business continuity, corporate transactions, and organizational governance.

4.6 Marketing and Communications

Send service-related communications and, where permitted, information about Agility products, services, events, or updates. You may unsubscribe from marketing emails using the link in the message or by contacting us. Opting out of marketing does not stop transactional, security, legal, or account-servicing communications.

5. How We Disclose Personal Information

We may disclose personal information to the following categories of recipients for the purposes described in this Policy:

5.1 Sponsor Banks and Program Partners

Applicable sponsor banks, program managers, ledger and payment-connectivity providers, and other banking partners that support account issuance, payment execution, settlement, program oversight, compliance, and servicing.

5.2 Financial Institutions and Payment Participants

Originating and receiving banks, correspondent and intermediary banks, payment networks, clearing systems, account-linking providers, liquidity providers, beneficiaries, counterparties, and other participants needed to execute or investigate a transaction.

5.3 Verification, Fraud, and Compliance Providers

Identity- and business-verification providers, fraud-prevention providers, sanctions and watchlist vendors, adverse-media and public-record providers, bank-account-verification providers, and other risk and compliance service providers.

5.4 Operational Service Providers

Cloud hosting, cybersecurity, communications, customer-support, document-management, data-storage, analytics, software, payment-processing, professional, audit, insurance, and other vendors that process information for Agility under contractual restrictions.

5.5 Authorities and Other Required Recipients

Regulators, government agencies, tax authorities, law enforcement, courts, arbitrators, and other parties when disclosure is required or permitted by law, legal process, regulatory direction, network rules, or a good-faith need to protect rights, safety, security, or the integrity of the financial system.

5.6 Professional Advisers and Corporate Transactions

Lawyers, accountants, auditors, insurers, consultants, financing sources, and parties involved in an actual or proposed merger, acquisition, financing, reorganization, sale of assets, insolvency, or similar transaction, subject to appropriate confidentiality and legal protections.

5.7 At Your Direction

Your authorized users, representatives, agents, recipients, or other parties when you direct or authorize the disclosure.

Service providers may use personal information only to perform services for Agility or as otherwise permitted by their contracts and applicable law. Other financial institutions and transaction participants may process information under their own legal obligations and privacy notices.

6. Sale, Sharing, and Targeted Advertising

Agility does not sell personal information for monetary consideration. We do not use sensitive personal information to infer characteristics about you or for purposes unrelated to providing, securing, and complying with legal requirements for the services. We may use analytics and similar technologies as described in Section 7. Certain U.S. state laws define “sale,” “sharing,” and “targeted advertising” broadly and may treat some disclosures involving non-essential analytics or advertising technologies as those activities even when no money is exchanged. Where applicable, we will provide the notice and method required to opt out of a sale, sharing, or targeted-advertising activity. We also disclose personal information to service providers, sponsor banks, financial institutions, payment participants, and other recipients for the operational, compliance, security, and transaction purposes described in this Policy. Those disclosures are generally made to provide or protect the services and are not treated as sales or targeted-advertising sharing except where applicable law provides otherwise.

7. Cookies and Similar Technologies

We and our service providers may use cookies, pixels, software development kits, local storage, and similar technologies to operate the website and platform, keep sessions secure, remember preferences, understand usage, diagnose problems, measure performance, and prevent fraud.

Where required, we provide a cookie-management tool that allows you to make choices about non-essential technologies. Browser settings may also allow you to block or delete cookies, although some service functions may not work properly. Where applicable law requires us to recognize an opt-out preference signal, such as Global Privacy Control, we will process the signal for the browser or device from which it is sent.

Because there is not yet a uniform industry response to browser “Do Not Track” signals, our services may not respond to those signals unless required by law.

8. Data Retention

We retain personal information for as long as reasonably necessary to provide and secure the services, maintain the customer relationship, complete transactions, resolve disputes, enforce agreements, prevent fraud, support audits, and meet legal, regulatory, tax, accounting, sponsor-bank, payment-network, and recordkeeping requirements.

Customer-identification, due-diligence, transaction, authorization, monitoring, and compliance records are generally retained for at least five years where required by applicable financial-crime or payment laws, and may be retained longer when another law, legal hold, investigation, dispute, contract, or regulator requires it. Retention periods vary by record type and are governed by Agility’s retention schedule. When information is no longer required, we delete, de-identify, or securely dispose of it in accordance with that schedule and applicable law.

9. Information Security

Agility maintains administrative, technical, and physical safeguards designed to protect personal information against unauthorized access, use, alteration, disclosure, loss, and destruction. These safeguards include access controls, authentication, encryption where appropriate, logging and monitoring, vulnerability and incident management, vendor oversight, staff training, business-continuity controls, and secure disposal practices.

No system or transmission method is completely secure. You are responsible for maintaining the confidentiality of your credentials, using appropriate device security, and promptly notifying us of suspected unauthorized access or fraud.

10. Your Privacy Rights and Choices

Depending on where you reside and subject to legal exceptions, you may have the following rights:

10.1 Access and Confirmation

Confirm whether we process your personal information and request access to categories or specific pieces of personal information we maintain about you.

10.2 Correction

Request correction of inaccurate personal information, taking into account the nature and purpose of the information.

10.3 Deletion

Request deletion of personal information, subject to exceptions for legal compliance, transaction completion, security, fraud prevention, disputes, and other permitted purposes.

10.4 Portability

Request a portable copy of certain personal information in a technically feasible format.

10.5 Opt-Out Rights

Opt out of the sale or sharing of personal information, targeted advertising, or certain profiling where those activities occur and the right applies. Instructions for exercising an applicable opt-out right will be provided through our website, cookie-management tool, or privacy-request process.

10.6 Sensitive Information

Limit or withdraw consent for certain processing of sensitive personal information where the law provides that right. This right does not prevent processing needed to provide requested services, verify identity, prevent fraud, secure accounts, or comply with law.

10.7 Appeal and Non-Discrimination

Appeal a decision on a privacy request where applicable and exercise privacy rights without unlawful discrimination, retaliation, or denial of service. We may still be unable to provide a financial service when required information is deleted, restricted, or not provided.

10.8 Marketing Choices

Unsubscribe from marketing communications at any time. You may also withdraw consent where processing is based on consent, but withdrawal does not affect prior processing and does not prevent processing required by law or contract.

To exercise a right, email privacy@agilityforex.com, call +1 (604) 484-2826, or write to the address in Section 15. Please describe your request and the state in which you reside. We will verify your identity using information reasonably related to the request. We will not ask you to provide more information than necessary, although additional verification may be required for sensitive records.

An authorized agent may submit a request where permitted by law. We may require proof of the agent's authority and may ask you to confirm the request directly. We will respond within the period required by applicable law. If we deny a request, we will explain the basis and any available appeal process.

11. Additional Information for California Residents

This section supplements the rest of this Policy for California residents. Some information that Agility processes may be exempt from the California Consumer Privacy Act because it is subject to the Gramm-Leach-Bliley Act or another exemption. Other personal information may remain subject to California law.

11.1 Categories Collected and Disclosed

During the preceding 12 months, Agility may have collected the following California categories of personal information: identifiers; customer-record information; protected classification characteristics; commercial and transaction information; internet or other electronic-network activity; approximate geolocation data; audio, electronic, visual, and similar information; professional or employment-related information; inferences; and sensitive personal information, including government identifiers, account access information, precise information if needed for fraud or security, and biometric information processed for identity verification.

The examples in Section 2 describe these categories in practical terms. The sources are described in Section 3, the business and commercial purposes in Section 4, and the categories of recipients in Section 5. Agility may disclose these categories for operational, compliance, security, transaction, legal, and business purposes. We do not knowingly sell or share the personal information of consumers under 16.

11.2 California Rights

Subject to applicable exceptions, California residents may request to know, access, correct, or delete personal information; obtain information about categories, sources, purposes, and recipients; opt out of sale or sharing; limit certain uses of sensitive personal information; access or opt out of certain automated decisionmaking uses where applicable; and receive equal service and pricing when exercising their rights.

Agility uses sensitive personal information only for purposes reasonably necessary to provide requested financial services; verify identity; prevent, detect, and investigate fraud and security incidents; comply with law; maintain service quality and safety; and perform other purposes permitted without a right to limit. Agility does not use sensitive personal information to infer characteristics.

Agility may use automated tools to assist identity, fraud, sanctions, compliance, eligibility, and transaction-risk reviews. These tools support, but do not replace, appropriate human review. Before any use that triggers a separate California notice, access right, or opt-out right, Agility will provide the required disclosure and process.

11.3 California Request Metrics and Authorized Agents

If California law requires Agility to publish annual privacy-request metrics, those metrics will be made available through the website. An authorized agent may submit a request as described in Section 10. We may require signed permission, evidence of registration with the California Secretary of State where applicable, and direct identity confirmation.

12. Children’s Privacy

Agility’s services are not directed to children under 13, and we do not knowingly collect personal information from children under 13. U.S. financial services are available only to persons who meet Agility’s eligibility and age requirements. If we learn that we collected a child’s personal information contrary to law, we will take appropriate steps to delete or otherwise address it.

13. Cross-Border Processing

Agility is based in Canada and provides services involving U.S. and international financial institutions, payment systems, counterparties, and service providers. Personal information may therefore be processed in Canada, the United States, and other countries where service providers or transaction participants operate. Privacy and government-access laws in those countries may differ from those in your state. Agility uses contractual, organizational, and technical measures designed to protect information in accordance with this Policy and applicable law.

14. Changes to This Policy

We may update this Policy to reflect changes in our services, technology, legal requirements, or information practices. We will post the updated Policy and revise the “Last updated” date. We will provide additional notice or obtain consent when required by law. Material changes will apply prospectively unless otherwise permitted.

15. Contact Us

Questions, complaints, and privacy requests may be directed to:

Privacy Officer / Data Protection
Agility Forex Ltd.
555 Burrard Street, Suite 15-105
Vancouver, British Columbia V7X 1M8
Canada
Email: privacy@agilityforex.com
Telephone: +1 (604) 484-2826