PRIVACY

Privacy Policy

Version eb2d397 · last updated 2026-07-01

Effective Date: June 19, 2026

This Privacy Policy describes how Frontline Prop collects, uses, discloses, and protects personal information in connection with our trader evaluation programs, funded trading accounts, website, and related services. We are committed to protecting your privacy and handling your data in accordance with applicable data protection laws, including the European Union General Data Protection Regulation ("EU GDPR"), the United Kingdom General Data Protection Regulation and Data Protection Act 2018 ("UK GDPR"), the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA/CPRA"), the Virginia Consumer Data Protection Act ("VCDPA"), the Colorado Privacy Act ("CPA"), the Connecticut Data Privacy Act ("CTDPA"), the Utah Consumer Privacy Act ("UCPA"), the Texas Data Privacy and Security Act ("TDPSA"), the Oregon Consumer Privacy Act ("OCPA"), the Montana Consumer Data Privacy Act ("MCDPA"), Brazil's Lei Geral de Proteção de Dados ("LGPD"), Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"), Australia's Privacy Act 1988, Singapore's Personal Data Protection Act 2012 ("PDPA"), and other applicable global privacy frameworks.

This Privacy Policy applies to all individuals who interact with FLP, including but not limited to: traders participating in evaluation programs, funded traders, prospective customers, website visitors, affiliate partners, employees, contractors, job applicants, and any other individuals whose personal information we process. It applies regardless of how you access our services, whether through our website, mobile applications, APIs, third-party integrations, or offline interactions.

WHO WE ARE

Frontline Prop operates as the data controller for the personal information described in this Privacy Policy, meaning we determine the purposes and means of processing your personal data. Our Data Protection contact is privacy@frontlineprop.com. If you have questions about this Privacy Policy or our data practices, you may contact us at info@frontlineprop.com or Frontline Prop LLC, 805 Greenwood Street, Evanston, IL 60201.

PERSONAL INFORMATION WE COLLECT

We collect and process various categories of personal information depending on your relationship with us (e.g., trader, prospect, affiliate partner, employee, contractor, or job applicant). The categories of personal information we collect include:

Contact Information

We collect your full name, email address, phone number, country of residence, signup source, and communication preferences. For employees and contractors, we may also collect home address, personal phone number, personal email, emergency contact information, and date of birth.

Financial Information

We collect financial information necessary for our services, including billing address, tokenized payment card details, transaction history, IP address, payout history, profit-and-loss data, and position history. For funded traders submitting payout requests, we collect bank account or cryptocurrency wallet addresses, tax identification numbers (where required for tax reporting), and payout amounts through our payout processor. For employees and contractors, we collect SSN/tax ID, bank account details, salary and compensation information, tax withholding forms, and direct deposit information.

Behavioral and Tracking Data

We collect trading account IDs, evaluation results, trading activity logs, position history, and profit-and-loss data generated through your use of our platform. We also collect IP addresses, cookie identifiers, browsing behavior, ad click data, UTM parameters, device information, browser type, operating system, session duration, page views, click patterns, referral URLs, and server logs.

Identity Verification and Compliance Data

We may collect identity verification data including full name, date of birth, nationality, government-issued identification (passport or driver's license), selfie or photograph, and proof of address. Our KYC vendor also provides PEP/sanctions screening results. This may include biometric data (selfie for identity matching) and information from which racial or ethnic origin may be inferable from identification documents.

Employment and Recruitment Data

For job applicants, we collect resumes and CVs, cover letters, employment and education history, professional references, interview notes, and assessment or test results. We do not use an applicant tracking system; applicant data is stored in Google Workspace.

Affiliate Information

For affiliate partners, we collect affiliate name, email, company name, payment details, referral tracking IDs, and commission history.

Customer Support Data

We collect support ticket content, chat transcripts, and account identifiers in connection with customer support interactions.

HOW WE COLLECT PERSONAL INFORMATION

We obtain personal information from the following sources:

Directly from you when you register for an account, purchase an evaluation, sign up for a funded trader program, submit a job application, or otherwise interact with our services. We also collect information through automated means, including trading activity logs, website analytics, cookies, and server logs generated through your use of our platform. Additionally, we receive information from third parties, including affiliate referral links, identity verification vendors, and professional references.

PURPOSES OF PROCESSING

We may process your personal information for the following purposes:

Trader Evaluation and Funded Account Management

We use your contact, financial, and behavioral data to assess your trading performance against program rules, manage the evaluation lifecycle, administer funded trader accounts, process profit-sharing payouts, and conduct ongoing risk monitoring.

Payment Processing

We process financial data to facilitate payment for evaluation purchases, manage refunds, prevent fraud, and process profit-sharing payouts to funded traders, including tax reporting obligations (e.g., 1099 forms).

Customer Relationship Management and Onboarding

We use your contact information to manage your account, communicate about our services, provide onboarding support, and segment users for support and marketing purposes.

Identity Verification and Compliance

We process identity and compliance data for KYC (Know Your Customer) verification, anti-money laundering compliance, sanctions screening, and fraud prevention.

Marketing and Advertising

We use contact and behavioral data for digital marketing, website analytics, advertising targeting, email campaigns, and conversion tracking.

Affiliate Program Management

We process affiliate information for commission tracking, payouts, and performance reporting.

Customer Support

We use your information to respond to inquiries, resolve issues, and improve our knowledge base and help center.

Internal Administration and Security

We process employee and contractor information for account management, access control, security monitoring, and internal communications.

Recruitment and Employment

We use applicant data for hiring evaluation and process employee and contractor data for payroll and tax reporting. We do not currently use a separate applicant tracking system or HRIS; employee and contractor records are maintained in Google Workspace. Payroll processing for contractors is handled through Riseworks.

Website Performance and Security

We collect technical and behavioral data to monitor website performance, maintain platform security, optimize user experience, and troubleshoot issues.

Transactional Communications

We use your contact information as a conduit for CRM-triggered communications regarding your account activity, including evaluation results and account status updates.

LEGAL BASES FOR PROCESSING

Where EU GDPR or UK GDPR applies, we process personal information based on the following legal grounds:

Consent

We rely on your consent for processing in connection with the trader evaluation program, including when you accept our terms and conditions at evaluation signup. We also rely on consent for funded trader program processing when you accept our funded trader agreement terms, and for KYC verification during funded trader onboarding.

Contractual Necessity

We process data where necessary for the performance of a contract with you, including payment processing for evaluation purchases, affiliate program management, and employee and contractor administration.

Legitimate Interest

We rely on legitimate interests for customer relationship management (direct marketing to existing customers and prospects who have engaged with our services), marketing communications, customer support, internal administration and security (protecting company systems and data through access controls and audit logging), and candidate evaluation. Our legitimate interest in KYC and compliance processing is the prevention of fraud, money laundering, and terrorist financing in financial services.

Legal Obligation

We process data to comply with legal obligations, including tax reporting and payroll requirements for profit-sharing payouts (such as 1099 forms) and employee and contractor compensation.

SPECIAL CATEGORY DATA

We process special category data (sensitive personal data) in limited circumstances. Our KYC and compliance processes may involve biometric data (selfie for identity matching), and racial or ethnic origin may be inferable from identification documents. We justify this processing on the basis of preventing fraud, money laundering, and terrorist financing in financial services. For employees and contractors, we process sensitive personal data such as SSN/tax ID for compliance with employment laws, including payroll processing and tax reporting.

AUTOMATED DECISION-MAKING

We employ automated decision-making in the following contexts:

We use automated rule-based evaluation to determine pass/fail results based on trading performance metrics during the evaluation program. We also use automated rule enforcement for funded account violations, including drawdown limits and position sizing. Additionally, our KYC vendor performs automated identity verification and sanctions/PEP screening.

Where automated decisions significantly affect you, you have the right to obtain human intervention, express your point of view, and contest the decision, as provided under applicable law.

DATA RETENTION

We retain personal information for the following periods:

Trader relationship data (contact and behavioral information) is retained for the duration of the trader relationship plus five years. Financial records related to funded trading, payouts, and tax reporting are retained for the duration of the funded relationship plus seven years. Transaction records from evaluation purchases are retained for seven years, while tokenized card data is retained per the applicable payment processor's retention policy. CRM and marketing data is retained until opt-out for marketing purposes. Employee and contractor payroll and tax records are retained for the duration of employment plus seven years. Employee and contractor contact information is retained for the duration of employment plus three years.

THIRD-PARTY RECIPIENTS

We share personal information with the following categories of third-party recipients:

Platform and Technology Providers

We use third-party vendors to host and operate our trading platform, provide customer relationship management services, deliver cloud infrastructure hosting and compute services, provide DNS management, content delivery, DDoS protection and web application firewall services, and support business email and internal productivity tools. We also use source code repository providers for development collaboration.

Payment Processors

We use third-party payment gateways to process payments for evaluation purchases and payout processors to facilitate profit-sharing distributions to funded traders and generate tax forms (such as 1099s).

Marketing and Analytics Partners

We engage marketing agencies to manage digital marketing campaigns, creative content, and advertising. We also use customer communication platforms to provide live chat support and host our help center, and analytics platforms for website analytics and conversion tracking.

Affiliate Platform Providers

We use third-party affiliate tracking platforms for referral management, commission calculation, and performance reporting.

Identity Verification and Compliance Vendors

We engage KYC and identity verification providers to perform identity verification, anti-money laundering compliance, and sanctions screening on our behalf.

Co-Marketing Partners

We may share limited referral data (such as trader name and email) and co-marketing performance metrics with strategic marketing partners in connection with joint promotional programs. Such partners operate as independent data controllers for the accounts they manage.

Email Service Providers

We use third-party email platforms for marketing email campaigns and email analytics, and for transactional email delivery (such as account notifications and CRM-triggered communications regarding evaluation results and account status).

Professional Services Providers

We may share data with outside legal counsel, accounting and bookkeeping providers, banking and financial institutions, and similar professional service providers as necessary for legal advice, tax preparation, financial reporting, business banking, and regulatory compliance.

Government and Regulatory Authorities

We may disclose personal information to governmental bodies, law enforcement agencies, courts, or regulatory authorities where required by law, legal process, or to protect our rights and the safety of others.

All processors and service providers engaged by us process personal data on our behalf and in accordance with our instructions, subject to data processing agreements and appropriate security measures. Where required by applicable law, a current list of our sub-processors is available in our Sub-processors list. We will update that list when we engage new sub-processors or replace existing ones, and where required, we will provide advance notice of such changes.

INTERNATIONAL DATA TRANSFERS

Where your personal data is transferred outside the jurisdiction in which it was collected, we implement appropriate safeguards in accordance with applicable data protection laws. Such safeguards may include Standard Contractual Clauses approved by the European Commission ("SCCs") or Binding Corporate Rules ("BCRs") for intra-group transfers.

DATA SECURITY

We implement appropriate technical and organizational measures to protect your personal information, including TLS encryption in transit, role-based access controls, multi-factor authentication on administrative accounts, tokenized payment credentials, PCI-DSS compliance for payment processing, web application firewall protections, encryption at rest and in transit, centralized identity and access management with single sign-on, and pseudonymized analytics where possible.

While we take commercially reasonable steps to protect your personal information, no method of transmission over the Internet or method of electronic storage is completely secure. We cannot guarantee the absolute security of your data. In the event of a personal data breach that poses a risk to your rights and freedoms, we will notify the relevant supervisory authority and, where required by applicable law, notify affected individuals without undue delay.

YOUR PRIVACY RIGHTS

Depending on your jurisdiction and applicable law, you may have the following rights regarding your personal information:

Right of Access

You may request confirmation of whether we process your personal information, and obtain a copy of the personal information we hold about you, together with supplementary information about the processing.

Right to Rectification / Correction

You may request correction of inaccurate or incomplete personal information.

Right to Erasure / Deletion

You may request deletion of your personal information, subject to legal retention requirements and applicable exceptions.

Right to Restrict Processing

You may request that we restrict the processing of your personal information in certain circumstances, including where you contest accuracy, where processing is unlawful, or where you have objected to processing.

Right to Data Portability

Where technically feasible and where processing is based on consent or contract and carried out by automated means, you may request to receive your personal information in a structured, commonly used, machine-readable format, or request direct transmission to another controller.

Right to Object

You may object to processing based on legitimate interests or for direct marketing purposes. Where you object to direct marketing, we will cease processing for that purpose without delay.

Right to Withdraw Consent

Where processing is based on consent, you may withdraw your consent at any time without affecting the lawfulness of processing prior to withdrawal.

Rights Related to Automated Decision-Making and Profiling

You may request human intervention in automated decisions that produce legal or similarly significant effects concerning you, express your point of view, and contest the decision.

Right to Opt Out of Sale, Sharing, or Targeted Advertising. Where applicable law provides, you may opt out of the sale or sharing of your personal information and of processing for purposes of targeted advertising or profiling.

Right to Limit Use of Sensitive Personal Information

Where applicable law provides, you may direct us to limit our use of sensitive personal information to purposes necessary to provide the services you have requested.

Right to Non-Discrimination / Non-Retaliation

We will not discriminate or retaliate against you for exercising any of your privacy rights.

Right to Appeal

If we decline your privacy request, you have the right to appeal our decision. We will provide instructions for submitting an appeal in our written response.

To exercise any of these rights, please contact us at info@frontlineprop.com. We will verify your identity and respond to verifiable requests within the timeframes required by applicable law. You may designate an authorized agent to submit requests on your behalf, subject to verification of the agent's authority and your identity.

CALIFORNIA PRIVACY NOTICE (CCPA/CPRA)

This section provides additional disclosures required under the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively, "CCPA"), and applies solely to California residents ("consumers"). This notice supplements the information contained elsewhere in this Privacy Policy.

Categories of Personal Information Collected

In the preceding twelve months, we have collected the following categories of personal information as defined by the CCPA:

Identifiers

Full name, email address, phone number, country of residence, signup source, mailing address, account name, trading account ID, IP address, affiliate tracking IDs, and tax identification numbers (where required for payouts).

Personal Information Under Cal. Civ. Code § 1798.80(e). Name, address, telephone number, financial information (bank account numbers, credit/debit card numbers in tokenized form, cryptocurrency wallet addresses), and employment history.

Characteristics of Protected Classifications Under California or Federal Law

Date of birth, nationality, and information that may reveal racial or ethnic origin as inferable from government identification documents submitted for KYC verification.

Commercial Information

Transaction history, evaluation purchase records, payout history, profit-and-loss data, commission history, and records of products or services purchased or considered.

Biometric Information

Selfie or photograph used for identity matching in connection with KYC verification processes.

Internet or Other Electronic Network Activity Information

Browsing behavior, ad click data, UTM parameters, cookie identifiers, device information, browser type, operating system, session duration, page views, click patterns, referral URLs, server logs, and trading activity logs.

Geolocation Data

Country of residence and IP-derived approximate location.

Professional or Employment-Related Information

Resume/CV, employment history, education history, professional references, interview notes, job title, role, and compensation data.

Inferences Drawn from Personal Information

Trading performance assessments, evaluation pass/fail determinations, risk profiles, marketing segmentation, and fraud risk indicators.

Sensitive Personal Information

Social Security number or tax identification number (for employees, contractors, and funded traders requesting payouts), bank account or cryptocurrency wallet details, government-issued identification (passport, driver's license), and biometric data (selfie for identity matching).

Business and Commercial Purposes for Collection

We collect personal information for the following business and commercial purposes: performing trader evaluation services; administering funded trading accounts and processing payouts; processing payments and preventing fraud; identity verification and compliance with legal obligations; marketing and advertising; affiliate program management; customer support; internal administration and security; recruitment and employment; and website performance optimization.

Sources of Personal Information

We collect personal information from the following categories of sources: directly from you; automatically through your use of our platform and website; from third-party service providers (e.g., identity verification vendors, payment processors); from referral partners and affiliates; and from publicly available sources.

Disclosure of Personal Information for Business Purposes

In the preceding twelve months, we have disclosed the following categories of personal information to our service providers and contractors for business purposes: identifiers; personal information under Cal. Civ. Code §1798.80(e); commercial information; internet or electronic network activity information; geolocation data; professional information; biometric information; inferences; and sensitive personal information. Recipients include platform and technology providers, payment processors, marketing and analytics partners, customer communication platforms, affiliate platform providers, identity verification and compliance vendors, email service providers, cloud infrastructure providers, and professional service providers.

Sale and Sharing of Personal Information

We do not "sell" personal information as defined by the CCPA for monetary consideration. We may "share" personal information (as defined under the CCPA) with advertising and analytics partners for purposes of cross-context behavioral advertising. The categories of personal information that may be shared include identifiers, internet or electronic network activity information, and inferences.

You have the right to opt out of the sharing of your personal information for cross-context behavioral advertising. To exercise this right, please contact us at info@frontlineprop.com or use the "Do Not Sell or Share My Personal Information" link on our website.

Use and Disclosure of Sensitive Personal Information

We use sensitive personal information only for purposes authorized under the CCPA, including: performing services on your behalf (identity verification, payment processing, payouts); ensuring security and integrity; short-term transient use; and complying with legal obligations. We do not use or disclose sensitive personal information for purposes of inferring characteristics about you beyond what is necessary to provide our services.

Retention of Personal Information

We retain each category of personal information for the periods described in the "Data Retention" section above, which are reasonably necessary for the disclosed purposes of collection, to comply with legal obligations, and to resolve disputes.

California Consumer Rights

As a California resident, you have the following rights under the CCPA:

Right to Know

You have the right to request that we disclose the categories and specific pieces of personal information we have collected about you, the categories of sources, the business or commercial purposes for collection, and the categories of third parties with whom we share personal information.

Right to Delete

You have the right to request deletion of personal information we have collected from you, subject to certain exceptions (e.g., legal obligations, completing transactions, exercising legal claims).

Right to Correct

You have the right to request that we correct inaccurate personal information we maintain about you.

Right to Opt Out of Sale/Sharing

You have the right to opt out of the sale or sharing of your personal information for cross-context behavioral advertising.

Right to Limit Use of Sensitive Personal Information

You have the right to limit our use of your sensitive personal information to purposes authorized by the CCPA.

Right to Non-Discrimination

We will not discriminate against you for exercising any of your CCPA rights.

To submit a request, please contact us at info@frontlineprop.com. We will verify your identity before processing your request. You may also designate an authorized agent to submit requests on your behalf, subject to verification of the agent's authority.

Financial Incentive Programs

We do not currently offer financial incentive programs that require CCPA disclosure. If we introduce such programs in the future, we will provide the required notices at that time.

U.S. STATE PRIVACY RIGHTS (ADDITIONAL STATES)

In addition to the rights described for California residents above, residents of Virginia, Colorado, Connecticut, Utah, Texas, Oregon, Montana, and other states with comprehensive consumer privacy laws may have similar rights, including:

Right to Access

You may request confirmation of whether we are processing your personal data and obtain a copy of such data.

Right to Delete

You may request deletion of personal data you have provided to us or that we have obtained about you.

Right to Correct

You may request correction of inaccuracies in your personal data.

Right to Data Portability

You may request your personal data in a portable, readily usable format.

Right to Opt Out

You may opt out of (i) targeted advertising, (ii) the sale of personal data (if applicable), and (iii) profiling in furtherance of decisions that produce legal or similarly significant effects.

Right to Appeal

If we decline your privacy request, you have the right to appeal our decision. We will provide instructions for submitting an appeal in our response to your request.

To exercise these rights, please contact us at info@frontlineprop.com. We will respond within the timeframes required by applicable state law. We do not require the creation of a new account to submit a privacy request.

COOKIES AND TRACKING TECHNOLOGIES

We use cookies and similar tracking technologies on our website. We obtain your consent for non-essential cookies through a cookie consent banner where required by law. For more information about the cookies we use and how to manage your preferences, please refer to our Cookie Policy.

DO NOT TRACK AND GLOBAL PRIVACY CONTROLS

Some browsers and devices transmit "Do Not Track" (DNT) signals or Global Privacy Control (GPC) signals. Where required by applicable law, we treat GPC signals as valid opt-out requests for the sale or sharing of personal information and for targeted advertising. We will honor GPC signals at the browser or device level for all users in jurisdictions where the law requires us to do so.

CHILDREN'S PRIVACY

Our services are not directed to children. We do not knowingly collect personal information from individuals under the age of 16 (or such other age as may be specified by applicable local law, including 13 in the United States for purposes of COPPA, and 13 in the United Kingdom). If we become aware that we have collected personal information from a child without appropriate parental or guardian consent, we will take steps to delete that information as promptly as practicable. If you believe we have inadvertently collected personal information from a child, please contact us immediately at info@frontlineprop.com.

UNITED KINGDOM ADDENDUM

This section applies to individuals located in the United Kingdom and supplements the information provided elsewhere in this Privacy Policy. Where the UK GDPR (the retained EU GDPR as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019) and the Data Protection Act 2018 apply, the following additional terms govern our processing of your personal data.

Data Controller

Frontline Prop is the data controller for the purposes of the UK GDPR and the Data Protection Act 2018. Our contact details are set out in the "Contact Us" section below.

Representative in the United Kingdom

If FLP is not established in the United Kingdom, our appointed representative in the UK for the purposes of Article 27 of the UK GDPR is: ADD CONTACT FOR UK REP IF REQUIRED.

Legal Bases for Processing

We process personal data of UK individuals on the same legal bases described in the "Legal Bases for Processing" section of this Privacy Policy (consent, contractual necessity, legitimate interests, and legal obligation). Where we rely on legitimate interests, we have conducted a balancing test to ensure that our interests are not overridden by your rights and freedoms.

International Transfers from the United Kingdom

Where we transfer personal data outside the United Kingdom, we ensure that appropriate safeguards are in place as required by UK data protection law. These safeguards may include: transfers to countries that have received an adequacy decision from the UK Secretary of State; the UK International Data Transfer Agreement ("UK IDTA"); the UK Addendum to the EU Standard Contractual Clauses; or Binding Corporate Rules approved by the UK Information Commissioner's Office ("ICO"). You may request a copy of the relevant transfer mechanism by contacting us at info@frontlineprop.com.

Your Rights Under UK Data Protection Law

In addition to the rights described elsewhere in this Privacy Policy, UK data subjects have the following rights under the UK GDPR and Data Protection Act 2018:

Right of Access (Subject Access Request). You have the right to obtain confirmation as to whether your personal data is being processed, and to access a copy of that data along with supplementary information about the processing.

Right to Rectification

You may request that we correct inaccurate personal data or complete incomplete personal data.

Right to Erasure (Right to Be Forgotten). You may request erasure of your personal data where there is no compelling reason for its continued processing, subject to certain exceptions.

Right to Restriction of Processing

You may request that we restrict processing of your personal data in certain circumstances, including where you contest accuracy or object to processing.

Right to Data Portability

Where processing is based on consent or contractual necessity and carried out by automated means, you have the right to receive your personal data in a structured, commonly used, machine-readable format.

Right to Object

You have the right to object to processing based on legitimate interests or for direct marketing purposes. Where you object to direct marketing, we will cease processing for that purpose immediately.

Rights Related to Automated Decision-Making and Profiling

You have the right not to be subject to a decision based solely on automated processing (including profiling) that produces legal or similarly significant effects, except where such processing is necessary for a contract, authorized by law, or based on your explicit consent. Where automated decisions are made regarding your trading evaluation or funded account status, you have the right to obtain human intervention, express your point of view, and contest the decision.

Right to Withdraw Consent

Where processing is based on your consent, you may withdraw consent at any time. Withdrawal does not affect the lawfulness of processing carried out prior to withdrawal.

Complaints to the Information Commissioner's Office

If you are located in the United Kingdom and are unsatisfied with our handling of your personal data or response to your rights request, you have the right to lodge a complaint with the UK Information Commissioner's Office (ICO):

Information Commissioner's Office Wycliffe House, Water Lane Wilmslow, Cheshire SK9 5AF Telephone: 0303 123 1113 Website: https://ico.org.uk/make-a-complaint/

Age of Consent for Online Services

Under UK law, we do not knowingly offer online services to individuals under the age of 13 without verifiable parental consent. Our services are not directed to individuals under the age of 18.

Direct Marketing and Electronic Communications

Where we send electronic marketing communications to UK individuals, we do so in compliance with the Privacy and Electronic Communications Regulations 2003 ("PECR"). We rely on the "soft opt-in" exemption for existing customers who have previously purchased or negotiated to purchase our services, and we provide an opportunity to opt out in every communication. For all other individuals, we obtain prior consent before sending marketing communications.

EUROPEAN ECONOMIC AREA ADDENDUM

This section applies to individuals located in the European Economic Area ("EEA") and supplements the information provided elsewhere in this Privacy Policy.

Representative in the EEA

If FLP is not established in the EEA, our appointed representative in the EEA for the purposes of Article 27 of the EU GDPR is: ADD CONTACT FOR EEA REP IF REQUIRED.

International Transfers from the EEA

Where we transfer personal data outside the EEA, we implement appropriate safeguards as required by the EU GDPR, including: transfers to countries with an adequacy decision by the European Commission; EU Standard Contractual Clauses (Module 1: Controller to Controller; Module 2: Controller to Processor); or Binding Corporate Rules. You may request a copy of the relevant safeguards by contacting us at info@frontlineprop.com.

Supervisory Authority

If you are located in the EEA and believe your data protection rights have not been adequately addressed, you have the right to lodge a complaint with your local supervisory authority. A list of EEA supervisory authorities is available at: https://edpb.europa.eu/about-edpb/about-edpb/members_en.

BRAZIL (LGPD) ADDENDUM

This section applies to individuals located in Brazil and supplements the information provided elsewhere in this Privacy Policy.

Under the Lei Geral de Proteção de Dados ("LGPD"), you have the following rights with respect to your personal data: confirmation of the existence of processing; access to your data; correction of incomplete, inaccurate, or outdated data; anonymization, blocking, or deletion of unnecessary or excessive data; portability of data to another service provider; deletion of data processed with consent; information about public and private entities with which data has been shared; information about the possibility of denying consent and the consequences thereof; and revocation of consent.

We process personal data of Brazilian individuals on the following legal bases under the LGPD: consent; compliance with a legal or regulatory obligation; legitimate interests (provided such interests do not override your fundamental rights and freedoms); execution of a contract or preliminary procedures related to a contract; and fraud prevention and credit protection.

To exercise your rights under the LGPD, please contact us at info@frontlineprop.com. We will respond within the timeframes required by applicable Brazilian law.

CANADA (PIPEDA) ADDENDUM

This section applies to individuals located in Canada and supplements the information provided elsewhere in this Privacy Policy.

Under the Personal Information Protection and Electronic Documents Act ("PIPEDA") and substantially similar provincial legislation (including Alberta's PIPA, British Columbia's PIPA, and Quebec's Law 25), you have the right to: access your personal information held by us; challenge its accuracy and have it amended; withdraw consent to our collection, use, or disclosure of your personal information (subject to legal or contractual restrictions); and file a complaint with the Office of the Privacy Commissioner of Canada or your applicable provincial privacy commissioner.

We collect, use, and disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances. Where required, we obtain meaningful consent before collecting, using, or disclosing personal information. We retain personal information only as long as necessary to fulfill the stated purposes or as required by law.

For Quebec residents, we will conduct a privacy impact assessment before disclosing personal information outside of Quebec and will ensure contractual safeguards are in place to provide substantially similar protection.

To exercise your rights or submit an inquiry, please contact us at info@frontlienprop.com.

AUSTRALIA (PRIVACY ACT 1988) ADDENDUM

This section applies to individuals located in Australia and supplements the information provided elsewhere in this Privacy Policy.

We handle personal information in accordance with the Australian Privacy Principles ("APPs") under the Privacy Act 1988 (Cth). We collect personal information only where reasonably necessary for our functions and activities, and by lawful and fair means. Where practicable, we collect personal information directly from you.

We will not use or disclose personal information for direct marketing unless you would reasonably expect us to do so or you have consented, and we provide a simple opt-out mechanism in every communication.

Before disclosing personal information to an overseas recipient, we take reasonable steps to ensure the recipient complies with the APPs or is subject to substantially similar protections.

You have the right to: access your personal information held by us; request correction of inaccurate information; and lodge a complaint with us or the Office of the Australian Information Commissioner (OAIC) if you believe we have breached the APPs.

To exercise your rights or submit a complaint, please contact us at info@frontlineprop.com.

SINGAPORE (PDPA) ADDENDUM

This section applies to individuals located in Singapore and supplements the information provided elsewhere in this Privacy Policy.

We comply with the Personal Data Protection Act 2012 ("PDPA") of Singapore in our collection, use, and disclosure of personal data. We will notify you of the purposes for which your personal data is collected, used, or disclosed, and obtain your consent unless an exception under the PDPA applies.

You have the right to: withdraw consent for our collection, use, or disclosure of your personal data (subject to legal or contractual consequences we will advise you of); request access to your personal data in our possession or under our control; and request correction of any errors or omissions in your personal data.

We will retain personal data only for as long as it is necessary to fulfill the purposes for which it was collected, or as required under applicable law. We implement reasonable security arrangements to protect personal data from unauthorized access, collection, use, disclosure, copying, modification, or disposal.

To exercise your rights, please contact us at info@frontlineprop.com. We will respond to access and correction requests within thirty (30) days, or such other period as required by the PDPA.

ADDITIONAL JURISDICTIONS

If you are located in a jurisdiction not specifically addressed above, we will process your personal information in accordance with the applicable data protection laws of your jurisdiction. Where local law provides you with additional or different rights than those described in this Privacy Policy, those local rights shall apply. We encourage you to contact us at info@frontlineprop.com if you have questions about how local law applies to your personal information.

CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time to reflect changes in our processing activities, legal requirements, or business practices. We will notify you of material changes by posting the updated policy on our website and updating the effective date above. Where required by applicable law, we will provide additional notice (such as an email notification or a prominent notice on our website) before changes take effect. We encourage you to review this Privacy Policy periodically.

CONTACT US

If you have questions, concerns, or complaints about this Privacy Policy or our data practices, please contact:

Frontline Prop LLC

Attn: Data Protection Officer

805 Greenwood Street

Evanston, IL 60201

Phone: (708) 581-6819

Email: privacy@frontlineprop.com

If you are located in the European Economic Area and believe that your data protection rights have not been adequately addressed, you have the right to lodge a complaint with your local supervisory authority. If you are located in the United Kingdom, you may contact the Information Commissioner's Office. If you are located in Australia, you may contact the Office of the Australian Information Commissioner. If you are located in Canada, you may contact the Office of the Privacy Commissioner of Canada or your applicable

provincial commissioner. If you are located in Singapore, you may contact the Personal Data Protection Commission. If you are located in Brazil, you may contact the Autoridade Nacional de Proteção de Dados (ANPD).