BREX CAPITAL

PRIVACY & DATA PROTECTION POLICY

Version 3.0 | 13 July 2026 | Confidential

www.brexcapital.com

compliance@brexcapital.com

BREX CAPITAL — PRIVACY & DATA PROTECTION POLICY (Version 3.0) Effective: 13 July 2026

Version: 3.0 **Effective Date:** 13 July 2026 **Supersedes:** All previous versions of the Brex Capital Privacy Policy and the Brex Capital Privacy, Security & Compliance Policy (December 2022) **Review Schedule:** Annual — next review due July 2027 **Data Controller:** Brex Capital LLC, and its group entities ("Brex Capital," "the Company," "we," "us") **Data Protection Officer (DPO):**dpo@brexcapital.com — appointed under PDPA Section 41(2) **Applies To:** All natural persons who are or have been Brex Capital clients, Introducing Brokers, Strategy Providers, or website visitors **Related Documents:** Brex Capital Trading & Compliance Policy (v3.0); Brex Capital Client Agreement; Brex Capital Cookie Notice **Lodge a Complaint:**dpo@brexcapital.com first; then the Thailand Personal Data Protection Committee (PDPC) at www.pdpc.or.th

Brex Capital LLC. Registration number: 457 LLC 2020. MISA licence T2023349. Email: compliance@brexcapital.com. Website: www.brexcapital.com.

THAILAND PDPA COMPLIANCE STATEMENT

This document is Brex Capital's Privacy and Data Protection Policy as required under the Thailand Personal Data Protection Act B.E. 2562 ("PDPA") and operates in conjunction with the Cybersecurity Act B.E. 2562 and the Royal Decree on Computer-Related Crimes (No. 2) B.E. 2568 (2025). It sets out how Brex Capital collects, uses, stores, protects, and processes personal data, and addresses the categories of PDPA obligations applicable to data controllers operating in or directing services to Thailand. Brex Capital has formally designated a Data Protection Officer (DPO) under PDPA Section 41(2) on the basis that Brex Capital qualifies as a financial-institution business

engaged in large-scale processing of personal data and regular monitoring of data subjects. Where Brex Capital processes personal data of individuals in the European Economic Area or United Kingdom, this Policy is designed to operate consistently with GDPR/UK GDPR principles; Section 8 (International Data Transfers) addresses cross- border handling.

DEFINED TERMS

Term	Meaning
Client	Any natural person who holds or has applied for a Brex Capital trading account.
Company / Brex Capital / We	Brex Capital LLC and its group entities.
Data Subject	The natural person to whom personal data relates.
DPO	The Data Protection Officer appointed under PDPA Section 41(2).
PDPA	The Thailand Personal Data Protection Act B.E. 2562.
PDPC	The Thailand Personal Data Protection Committee, the PDPA regulator.
Personal Data	Any information relating to an identified or identifiable natural person, per PDPA Section 6.
Sensitive Personal Data	The categories listed at PDPA Section 26, including biometric and financial data (Section 6 below).
Trading & Compliance Policy	The related Brex Capital policy cross-referenced at Section 15.

1. WHO WE ARE AND HOW TO CONTACT US

1.1 Data Controller

Brex Capital is the Data Controller for all personal data collected and processed in connection with Brex Capital trading accounts, Introducing Broker partnerships, Strategy Provider activities, and website usage. As Data Controller, Brex Capital determines the purposes and means of processing personal data within the meaning of the PDPA.

1.2 Data Protection Officer — Mandatory Appointment

In accordance with PDPA Section 41(2) and the PDPC Notification on Designation of Data Protection Officers (effective 13 December 2023), Brex Capital has formally designated a DPO on three independent grounds: (a) Brex Capital engages in the regular and large-scale monitoring of data subjects (trade-pattern monitoring, behavioral analytics, fraud prevention); (b) Brex Capital qualifies as a financial-institution business under the PDPC's sectoral notification; and (c) Brex Capital processes sensitive personal data within the meaning of PDPA Section 26, including biometric data collected during identity verification.

The DPO advises Brex Capital on PDPA compliance, monitors policy adherence, coordinates with the PDPC, and serves as the point of contact for data-subject inquiries.

1.3 Contact Details

Function	Contact
General Enquiries	support@brexcapital.com
Data Protection Officer (DPO)	dpo@brexcapital.com
Compliance Department	compliance@brexcapital.com
Security Incidents	security@brexcapital.com

Function	Contact
Complaints	complaints@brexcapital.com
Website	www.brexcapital.com
Thailand PDPC (Regulator)	www.pdpc.or.th

1.4 Language

This Policy is published in English and Thai. Both versions are equally authoritative. Where a discrepancy arises between them, the Thai version prevails where required by Thai law; otherwise the English version prevails. The Thai version is available at www.brexcapital.com/privacy and on request from dpo@brexcapital.com.

2. WHAT PERSONAL DATA WE COLLECT

2.1 Categories of Personal Data

Brex Capital collects and processes the following categories, limited to what is necessary for the purposes at Section 3 (data minimization):

Category	Examples	Source
Identity Data	Full legal name, date of birth, nationality, passport or national ID number, photograph.	Provided by client at registration
Contact Data	Email, phone number, residential and postal address.	Provided by client at registration

Category	Examples	Source
Financial Data	Bank account details, deposit/withdrawal history, account balance, trading history. (Sensitive — see Section 6.)	Provided by client; generated by trading activity
Document Data	Copies of passport, national ID, driving licence, proof of address, bank statements, source-of-wealth documents.	Provided by client for KYC
Biometric Data	Selfie images and short videos collected during identity verification; facial geometry derived from such images for liveness and matching checks. (Sensitive — see Section 6.)	Provided by client at registration, with explicit consent, where the client elects this verification method
Technical Data	IP address, device fingerprint, device ID, MT5 Terminal ID, browser type, operating system, login timestamps, session data.	Collected automatically

Category	Examples	Source
Trading Data	All orders including cancelled and executed trades, position history, MT5 account ID, leverage used, profit and loss records.	Generated by trading activity
Communication Data	Email and chat with Brex Capital, support-ticket content, call recordings where applicable.	Generated by client interactions
Compliance Data	KYC status, AML screening results, sanctions-check results, compliance investigation notes, Politically Exposed Person (PEP) status.	Generated by compliance processes
Marketing Data	Marketing preferences, promotion participation history, referral source.	Provided by client or collected at registration

Category	Examples	Source
Monitoring Data	IP logs, device logs, trade-pattern analysis outputs, Client ID cross-reference records, Expert Advisor activity logs, behavioral ML/AI pattern-detection outputs, cross-account correlation results.	Generated by compliance monitoring

2.2 Sensitive Personal Data — PDPA Section 26

Certain categories above fall within "sensitive personal data" under PDPA Section 26 and require explicit consent. Section 6 of this Policy sets out Brex Capital's specific treatment of sensitive personal data, including biometric and financial data.

2.3 Data We Do Not Collect

Brex Capital does not collect payment-card PIN numbers, banking passwords, or full payment-card numbers (only a masked reference token is retained), and does not collect special-category data for which it has no operational need — including political opinions, religious or philosophical beliefs, sexual behavior, genetic data, or trade-union membership — except where required by law. Clients should never share passwords or PINs with any party, including anyone purporting to represent Brex Capital.

2.4 Data Minimization

Brex Capital collects only personal data that is adequate, relevant, and limited to what is necessary for the purposes set out in this Policy, and periodically reviews its collection practices to remove fields no longer required.

3. LEGAL BASIS FOR PROCESSING

Under the PDPA, Brex Capital must have a valid legal basis under Sections 24 (general personal data) and 26 (sensitive personal data) for each processing activity:

Processing Activity	Legal Basis (PDPA)	Details
Account registration and KYC	Contractual necessity plus legal obligation (Sections 24(3), 24(6))	Required to enter and fulfil the client agreement; also required by AML law.
Identity verification (documentary and/or biometric — see Section 6)	Explicit consent for the biometric element (Section 26); contractual necessity plus legal obligation for identity verification generally	Identity verification is a regulatory prerequisite for account opening. Clients choose between a documentary-plus-supervised-video path or a biometric path; see Section 6.2.
Processing deposits and withdrawals	Contractual necessity (Section 24(3))	Required to perform payment services under the client agreement.
Executing and recording trades	Contractual necessity (Section 24(3))	Required to perform the core trading service.
AML screening and sanctions checks	Legal obligation (Section 24(6))	Required under Thailand AMLO regulations and applicable international sanctions obligations.

Processing Activity	Legal Basis (PDPA)	Details
IP, device, and trade-pattern monitoring	Legitimate interest plus contractual consent (Sections 24(5), 24(3))	Fraud and Prohibited Practice prevention; client provides explicit consent at account opening.
Behavioral ML/AI pattern detection	Legitimate interest (Section 24(5))	Detection of automated systems, AI Analysis Software, and platform-exploitation patterns.
Cross-account correlation analysis	Legitimate interest (Section 24(5))	Detection of coordinated trading rings and multi-account abuse.
Same-IP / Same-Device aggregation	Legitimate interest (Section 24(5))	Aggregation of orders from shared identifiers for fraud prevention; see the Trading & Compliance Policy §4.4.
Marketing communications	Consent (Section 19)	Sent only where the client has opted in; consent may be withdrawn at any time.
Regulatory reporting and SARs	Legal obligation (Section 24(6))	Required under AML and financial-regulation obligations.

Processing Activity	Legal Basis (PDPA)	Details
Compliance investigations	Legitimate interest plus legal obligation	Protecting Brex Capital's business and meeting legal obligations to investigate suspected Prohibited Practices.
Record retention	Legal obligation (Section 24(6))	Required by financial regulation, AML law, and PDPA recordkeeping rules.

4. HOW WE USE YOUR PERSONAL DATA

4.1 Primary Purposes

Brex Capital uses personal data to: open and manage trading accounts; verify identity and conduct KYC checks (documentary and/or biometric, per client choice — Section 6); process deposits, withdrawals, and other financial transactions; execute and maintain trading-activity records; provide customer support; conduct AML/CTF and sanctions compliance checks; monitor trading activity for compliance with the Trading & Compliance Policy, including behavioral ML/AI pattern detection, cross-account correlation analysis, and Same-IP/Same-Device aggregation; administer the Social Trading platform and calculate Strategy Provider fees; communicate account- related information including policy changes; and investigate and enforce the Trading & Compliance Policy.

4.2 Secondary Purposes — With Consent Only

With separate, granular, and revocable consent, Brex Capital may use personal data to send marketing communications about Brex Capital products, promotions, and events, to conduct client-satisfaction surveys, and to invite

participation in research panels. Any of these consents may be withdrawn independently at any time without affecting the client's account.

4.3 Automated Decision-Making and Profiling

Brex Capital uses automated systems for: sanctions-list screening; trade-pattern flagging against Prohibited Practices defined in the Trading & Compliance Policy §5; margin and stop-out calculation; behavioral ML/AI pattern detection; and cross-account correlation analysis.

Human review guarantee. No significant compliance decision affecting a client's account — suspension, restriction, termination, fee imposition, or claw-back — is taken solely on the basis of automated processing. Every such decision is reviewed by a qualified compliance officer before action. Clients may request human review of any automated flag that resulted in an enforcement action by emailing dpo@brexcapital.com.

5. YOUR RIGHTS UNDER THE THAILAND PDPA

Under the PDPA, data subjects have the following eight rights. All requests go to dpo@brexcapital.com. Brex Capital responds within 30 days and may request additional information to verify identity before processing a request.

Right	What It Means	Limitations
Access	Request a copy of all personal data Brex Capital holds, including account data, KYC records, trade history, communication records, and monitoring data.	Brex Capital may redact third-party information or withhold data where disclosure would prejudice an active investigation or legal proceedings.

Right	What It Means	Limitations
Rectification	Correct inaccurate or incomplete data, including contact details, name changes, and errors.	Identity-related corrections require re-verification of identity documents.
Erasure	Request deletion where data is no longer needed for the original purpose, consent is withdrawn, or data was unlawfully processed.	Cannot be fulfilled where Brex Capital has a legal obligation to retain data (such as 7-year AML retention). Erasure of trading records is not possible for live or recently closed accounts.
Restriction	Request that Brex Capital restrict processing — for example, while a rectification request is assessed or accuracy is contested.	Restriction may delay Brex Capital's ability to process withdrawals or maintain active account services.
Data Portability	Request a copy, in structured machine-readable form, of data provided based on contractual necessity or consent.	Applies only to data the client provided; does not apply to data Brex Capital generated (compliance investigation notes, monitoring outputs).

Right	What It Means	Limitations
Object	Object to processing based on legitimate interest, including the monitoring activities in Section 4.3.	Objecting to compliance monitoring may prevent Brex Capital from offering trading services, as monitoring is necessary for policy enforcement and fraud prevention.
Withdraw Consent	Withdraw consent-based processing (marketing, or biometric verification if that path was chosen) at any time by emailing dpo@brexcapital.com or updating preferences in the Brex Capital portal.	Withdrawal does not affect the lawfulness of processing before withdrawal. Withdrawing consent to mandatory compliance monitoring, or to biometric verification without adopting the alternative path, may require account closure.
Complain	Submit a complaint to the PDPC at www.pdpc.or.th.	Clients are encouraged to first raise the complaint with the DPO at dpo@brexcapital.com before escalating.

How to exercise your rights. Email dpo@brexcapital.com with full name, account number, and a clear description of the request. Requests concerning sensitive personal data may require identity verification by a secondary channel (such as a video call). Brex Capital responds within 30 days,

extendable once by a further 30 days for complex requests, with prior written notice to the data subject.

6. SENSITIVE PERSONAL DATA AND BIOMETRIC DATA

6.1 PDPA Section 26 — Categories of Sensitive Data

Under PDPA Section 26, the following are treated as sensitive personal data and require explicit consent (or a specific statutory exception): racial or ethnic origin; political opinions; cult, religious, or philosophical beliefs; sexual behavior; criminal records; health data; disability; trade-union information; genetic data; biometric data; and financial information (as confirmed by the PDPC for regulated financial sectors).

6.2 Identity Verification — Biometric Verification Is Optional

Identity verification is mandatory before an account can be opened; it is required by AML law and by Brex Capital's regulatory obligations. **The verification method is a client choice.** Brex Capital offers two equivalent paths:

(a) Biometric verification — a selfie image and a short liveness video, processed to derive facial geometry data for matching against the client's submitted identity document, with re-verification permitted where

required under the Trading & Compliance Policy §7.3; or

(b) Documentary verification — submitted identity and address documents together with a supervised video call with a Brex Capital compliance officer, with no biometric data collected.

A client who declines biometric verification is not blocked from opening an account: Brex Capital offers the documentary-plus-supervised-video path in (b) as a full alternative. Declining biometric verification has no effect on account approval where the client completes path (b) to Brex Capital's standard identity-verification satisfaction. Consent for the biometric path (a), where chosen, is collected separately from general account-opening consent, and no financial inducement is offered for choosing it, as this would invalidate consent under PDPC guidance.

6.3 Biometric Data — Specific Safeguards

Where a client chooses biometric verification, Brex Capital applies:

(a) Explicit consent — collected via a consent screen identifying the type of biometric data, the purpose, the retention period, and the consequence of withdrawal.

(b) Purpose limitation — biometric data is used solely for identity verification and AML compliance; never for marketing, profiling, behavioral advertising, or any secondary purpose.

(c) Storage and encryption — stored separately from other client data, encrypted at rest with AES-256,

accessible only to compliance personnel performing verification tasks.

(d) Vendor governance — any third-party biometric verification provider is bound by a Data Processing

Agreement prohibiting use of Brex Capital clients' biometric data for any purpose other than the instructed

verification task.

(e) Right to withdraw — clients may withdraw consent for biometric processing at any time by emailing

dpo@brexcapital.com. Withdrawal does not affect the lawfulness of prior processing. A client who withdraws

biometric consent may complete or switch to the documentary path in Section 6.2(b) to keep the account active; account closure is required only if the client declines both verification paths.

6.4 Financial Data as Sensitive Personal Data

Financial information processed by regulated financial institutions falls within the scope of sensitive personal data. Brex Capital applies the same elevated safeguards to financial data (bank account details, deposit and withdrawal history, account balance, trading P&L) as to other sensitive personal data,

including explicit consent at account opening, encryption at rest, restricted access, and the data-subject rights at Section 5.

7. WHO WE SHARE YOUR DATA WITH

7.1 Categories of Recipients

Every external recipient (other than government authorities acting under legal compulsion) is subject to a written Data Processing Agreement obliging data-protection standards at least equivalent to the PDPA:

Recipient	Purpose	Basis
Liquidity Providers	Execution of client orders; limited to trade data required for execution.	Contractual necessity
Payment Processors	Processing deposits and withdrawals; limited to payment details required for the transaction.	Contractual necessity
KYC and Identity Verification Providers	Identity checks, document verification, and (where the client chooses that path) biometric matching, under DPAs.	Legal obligation plus contractual necessity
Sanctions Screening Providers	Screening client names and identifiers against international sanctions lists.	Legal obligation

Recipient	Purpose	Basis
IT and Cloud Service Providers	Hosting, maintenance, and security of Brex Capital systems, subject to strict DPAs with security audit rights.	Legitimate interest
External Auditors	Annual financial and security audits; read-only, limited scope.	Legitimate interest plus legal obligation
Financial Commission (FinCom)	Only where a client dispute has been formally submitted to FinCom.	Legitimate interest plus legal proceedings
Regulatory Authorities and Law Enforcement	Where required by law, court order, or regulatory request, including SAR filings with the Thailand AMLO.	Legal obligation
Introducing Brokers (IBs)	Only with client consent, limited to account-opening confirmation and basic account status; no trading data, financial details, or sensitive personal data.	Consent plus contractual necessity

7.2 No Sale of Personal Data

Brex Capital does not sell personal data to any third party for any commercial purpose, does not allow third-party advertisers, data brokers, or affiliate networks to access client personal data, and does not permit retargeting of client personal data for any third-party advertiser's benefit.

7.3 Data Processor Obligations

All Brex Capital data processors are required, under their Data Processing Agreements, to: process personal data only on documented Brex Capital instructions; implement technical and organizational security measures equivalent to Section 10 of this Policy; engage sub-processors only with Brex Capital's prior written authorization; notify Brex Capital without undue delay, and in any event within 24 hours of becoming aware, of any personal data breach; return or delete all personal data on termination of the DPA; and submit to audits and inspections by Brex Capital or its mandated auditor.

8. INTERNATIONAL DATA TRANSFERS

8.1 Transfer Safeguards — PDPA Sections 28 and 29

Brex Capital may transfer personal data outside Thailand in connection with its operations. Where the destination jurisdiction has not been recognized by the PDPC as providing adequate data protection, one of the following safeguards applies: Standard Contractual Clauses approved by the PDPC (or equivalent SCCs recognized under Section 28); Binding Corporate Rules for transfers within the Brex Capital group; explicit, informed, unambiguous consent for a specific one-time transfer with full disclosure of the recipient jurisdiction and risks; necessity for performance of the contract with the data subject (such as transferring trade data to a non-Thai liquidity provider to execute an order); or necessity for compliance with a legal obligation (such as a transfer under a mutual legal assistance treaty).

8.2 Liquidity Providers and Payment Processors

Brex Capital's liquidity providers and payment processors may be located outside Thailand. All are required, as a condition of their DPA, to apply data-protection standards at least equivalent to the PDPA. Brex Capital maintains a register of data processors and their applicable safeguards.

8.3 Cross-Border Transfer Inventory

A list of jurisdictions to which Brex Capital may transfer personal data, with the applicable safeguard, is available on request from dpo@brexcapital.com and is updated at least quarterly.

9. DATA RETENTION

9.1 Retention Schedule

Brex Capital retains personal data only as long as necessary for the purpose collected, or as required by law. At the end of the retention period, data is permanently deleted from all Brex Capital systems, including backups. This schedule aligns with the Trading & Compliance Policy §13:

Data Category	Retention Period	Reason
Identity and KYC documents	7 years from account closure	AML regulations, PDPA recordkeeping
Identity-verification data (biometric, where chosen, or documentary/video-call records)	Until verification is completed, plus 7 years from account closure	AML regulations, dispute resolution
Full trade history	7 years from account closure	Regulatory requirement, dispute resolution
Financial transaction records	7 years from account closure	AML law, accounting obligation

Data Category	Retention Period	Reason
Account communication records	7 years from account closure	Dispute resolution, regulatory compliance
Compliance investigation records	7 years from conclusion	Legal proceedings preparation
Suspicious Activity Reports (SARs)	7 years from filing	AML legal obligation — must not be deleted
Monitoring logs (IP, device, trade pattern, ML/AI outputs)	7 years from account closure	PDPA compliance monitoring basis, legal proceedings
Marketing preferences and consent records	Until consent withdrawn, plus 3 years	Proof of consent under PDPA
Social Trading performance data	7 years from last activity	Contractual plus regulatory records
Website analytics (anonymized)	2 years	Legitimate interest — anonymized, cannot identify individuals
Security incident records and breach register	10 years from incident closure	Regulatory reporting and post-incident review

9.2 Deletion Procedure

At the end of the retention period, personal data is deleted from production systems within 30 days and from encrypted backup storage on the next scheduled backup rotation cycle (no longer than 90 days). Deletion is logged and verifiable. SAR filings and other records subject to mandatory non-deletion obligations under AML law are retained beyond 7 years only to the extent legally required.

10. DATA SECURITY OVERVIEW

Brex Capital protects personal data with layered technical and organizational safeguards — encryption in transit and at rest, role-based access control, mandatory multi-factor authentication for staff and clients, independent penetration testing, and a tested incident-response plan. The full technical and organizational control set is set out in the **Internal Security Annex** at the end of this Policy; that annex is an internal operating standard and not a client-facing warranty of specific technical performance.

10.1 Mandatory Two-Factor Authentication for Clients

All Brex Capital client accounts are required to enable two-factor authentication (2FA) on the trading portal and, where supported, on the MT5 platform. Accounts that have not enabled 2FA within 30 days of opening will be restricted from initiating withdrawals until 2FA is activated. This is a security minimum, not an optional convenience.

10.2 Client Responsibilities

Clients are responsible for the security of their own account credentials and must: use a strong, unique password of at least 12 characters mixing upper case, lower case, digits, and symbols; never share login credentials with any third party, including anyone claiming to represent Brex Capital; notify Brex Capital immediately at security@brexcapital.com if unauthorized account access is suspected; and not access Brex Capital services from shared or public devices without clearing all session data on logout.

11. DATA BREACH NOTIFICATION

11.1 Brex Capital Obligations

Where a personal data breach is likely to result in a risk to the rights and freedoms of natural persons, Brex Capital follows this procedure:

Timeframe	Action
Within 24 hours of detection	Internal escalation to the DPO and the Chief Compliance Officer; containment measures and forensic preservation begin.
Within 72 hours of becoming aware	Notification to the PDPC, including nature of the breach, categories and approximate number of affected data subjects, DPO contact details, likely consequences, and measures taken or proposed.
Without undue delay	Direct notification to affected data subjects where the breach is likely to result in high risk to their rights and freedoms, covering what happened, what data was involved, what Brex Capital is doing about it, and what steps the individual can take.
Within 14 days	Coordinated notification to affected data processors, liquidity providers, payment processors, and Introducing Brokers.
Ongoing	Documentation in Brex Capital's breach register; post-incident review by the DPO and implementation of required improvements.

11.2 Incident Severity Classification

Severity	Criteria	Notification
Critical	Unauthorized disclosure of sensitive personal data (biometric, financial) affecting any data subject, or unauthorized access to client funds.	PDPC, affected data subjects, law enforcement (where applicable)
High	Unauthorized disclosure of non-sensitive personal data affecting more than 100 data subjects, or any disclosure of identity documents.	PDPC, affected data subjects
Medium	Unauthorized disclosure of non-sensitive personal data affecting fewer than 100 data subjects, with no biometric, financial, or identity-document content.	PDPC notification at Brex Capital's discretion based on risk assessment; affected data subjects notified
Low	Internal access-control violation or near-miss with no actual data disclosure.	Internal documentation only; reviewed in quarterly compliance report

11.3 Reporting a Suspected Breach

Clients who believe their account data has been compromised should: contact security@brexcapital.com with subject line "SECURITY INCIDENT"; change their account password immediately via the Brex Capital portal; enable 2FA if not already active; and preserve, not delete, suspicious emails, messages, or screenshots for forensic investigation. Clients should not take public action (such as social-media posts) regarding a suspected breach until Brex Capital has confirmed receipt and provided initial guidance, as premature public statements may impede investigation or escalate harm to other affected clients.

12. COOKIES AND WEBSITE DATA

12.1 Cookie Types

The Brex Capital website uses the following cookie categories. In accordance with PDPC guidance on consent, the cookie banner offers "Accept all" and "Reject all" with equal prominence, with granular sub-category consent available:

Cookie Type	Purpose	Can Be Disabled?
Strictly Necessary	Session management, login, security, fraud prevention. Cannot be disabled without breaking the site.	No
Functional	Remembering preferences, language settings, login state across sessions.	Yes — via cookie preferences

Cookie Type	Purpose	Can Be Disabled?
Analytics	Understanding website usage; data is aggregated and anonymized.	Yes — opt-in required
Marketing	Tracking effectiveness of Brex Capital advertising campaigns. Active only with consent.	Yes — opt-in required

12.2 Consent Logging

All cookie consent decisions are logged with a timestamp and stored as evidence of consent for a minimum of 3 years after the consent expires or is withdrawn, per PDPA recordkeeping obligations. Full cookie inventory and management interface: Brex Capital Cookie Notice, available at www.brexcapital.com/cookies.

13. CHILDREN'S PRIVACY

Brex Capital's trading services are not directed at, and are not lawfully available to, persons under the age of 20 years (the age of majority under the Thai Civil and Commercial Code). Brex Capital does not knowingly collect personal data from, or open trading accounts for, anyone under the age of 20.

13.1 PDPA Minor Consent Framework

Where personal data is collected from a minor, consent is governed by the Civil and Commercial Code Section 27: for persons under 10, consent must be obtained from the holder of parental authority in all cases; for persons 10 to 20 (and not sui juris by marriage or capacity), consent must be obtained both from the minor and the holder of parental authority, except for acts the minor

may perform independently under the Civil and Commercial Code; for persons 20 and above, the individual's own consent is sufficient.

13.2 Account Opening — Minimum Age 20

Notwithstanding the minor consent framework above, Brex Capital does not open trading accounts for persons under 20 regardless of parental consent, because: (i) trading activity carries financial risk; (ii) margin trading involves obligations minors are not legally capable of incurring under Thai law; and (iii) AML and tax reporting obligations apply to the account holder personally.

13.3 If We Become Aware

If Brex Capital becomes aware that personal data has been collected from a person under 20 without the required consent, that data will be deleted as soon as reasonably practicable, any related trading account will be closed, and any account funds will be returned to their originating source in accordance with applicable AML rules. Anyone who believes Brex Capital may hold data of a minor should contact dpo@brexcapital.com immediately.

14. DATA PROTECTION IMPACT ASSESSMENT AND VULNERABILITY DISCLOSURE

14.1 Data Protection Impact Assessment (DPIA)

Although the PDPA does not currently mandate DPIAs, Brex Capital conducts them as a matter of best practice before any new processing activity likely to result in high risk to data subjects' rights and freedoms. DPIAs are triggered automatically by: any new processing of biometric or other sensitive personal data under Section 26; any new automated decision-making or profiling system with potentially significant effects on data subjects; any new large-scale behavioral-data monitoring, including ML/AI pattern-detection systems; any new cross-border transfer arrangement involving sensitive personal data; and any material change to a data-processor relationship or the categories of data shared with one. Each DPIA is reviewed by the DPO and signed off by the Chief Compliance Officer before the relevant activity commences. DPIA records are retained for 7 years.

14.2 Vulnerability Disclosure and Security Research

Brex Capital welcomes responsible security research. Researchers who identify potential vulnerabilities should:

(a) Report channel — email security@brexcapital.com with subject line "VULNERABILITY DISCLOSURE," including a description of the vulnerability, reproduction steps, the affected system or URL, and any proof-of-concept that does not involve any Brex Capital client's personal data.

(b) Good-faith safe harbour — Brex Capital will not pursue legal action against a researcher who: acts in good faith; does not access, modify, or exfiltrate any client's personal data beyond what is strictly necessary to demonstrate the vulnerability; does not publicly disclose the vulnerability before Brex Capital has had a reasonable opportunity to remediate it (90 days unless otherwise agreed); and does not attempt to disrupt Brex Capital services or hold them to ransom.

(c) Response commitment — Brex Capital will acknowledge receipt within 2 business days, provide an initial assessment within 10 business days, and provide regular updates until resolution.

15. CROSS-REFERENCE TO RELATED BREX CAPITAL POLICIES

This Policy operates alongside the following Brex Capital policies. In the event of inconsistency, this Policy prevails on matters of personal data protection; the relevant other policy prevails on its own subject matter:

Related Policy	Subject Matter
Brex Capital Trading & Compliance Policy (v3.0)	Trade execution, prohibited practices, enforcement, monitoring and client consent, Same-IP/Same-Device aggregation, KYC standards, AML, deposits and withdrawals, slippage compensation, incident claims, set-off rights, record retention, sanctions, IB obligations, copy trading.

Related Policy	Subject Matter
Brex Capital Cookie Notice	Detailed cookie consent options, cookie inventory, cookie management interface (www.brexcapital.com/cookies).
Brex Capital Client Agreement	Contractual terms governing the trading relationship, including dispute resolution and limitation of liability.

16. LIMITATION AND SCOPE

This Policy addresses the collection, use, and protection of personal data. It does not constitute investment advice, a guarantee of trading outcomes, or a warranty regarding the performance of any Brex Capital system or third- party processor. Nothing in this Policy limits a data subject's non-waivable statutory rights under the PDPA. Disputes concerning the trading relationship itself (as opposed to data protection) are governed by the Brex Capital Client Agreement and resolved through FinCom, as referenced there.

17. UPDATES TO THIS POLICY

Brex Capital reviews and updates this Policy at least annually, with the next scheduled review in July 2027. Material changes will be notified to all active clients by email at least 14 days before the change takes effect. The updated Policy will be published at www.brexcapital.com/privacy. Continued use of Brex Capital services after the effective date constitutes acceptance of the updated Policy.

Where a change introduces a new processing activity requiring additional consent (such as a new identity- verification method), Brex Capital will request fresh explicit consent before that processing commences for existing clients.

Field	Value
Version	3.0

Field	Value
Effective Date	13 July 2026
Next Review Due	July 2027
Data Controller	Brex Capital and its group entities
Data Protection Officer (DPO)	dpo@brexcapital.com
Security Incidents	security@brexcapital.com
Complaints	complaints@brexcapital.com
Thailand PDPC	www.pdpc.or.th
Related Documents	Brex Capital Trading & Compliance Policy v3.0

— END OF BREX CAPITAL PRIVACY AND DATA PROTECTION POLICY (CLIENT-FACING) —