PRIVACY POLICY

How we collect, use, share and retain personal data

Bursa Prime Ltd. (trading as **BursaPrime**)

Registered in St. Lucia under number 2026-00616

Document: Privacy Policy

Version: 1.0

Owner: [Data Protection Officer / Compliance Department]

RISK WARNING

> **CFDs are complex instruments and come with a high risk of losing money rapidly due to leverage. 65% of retail investor accounts lose money when trading CFDs with this provider. You should consider whether you understand how CFDs work and whether you can afford to take the high risk of losing your money.**

TABLE OF CONTENTS

1. ABOUT THIS POLICY

1.1. This Privacy Policy explains how Bursa Prime Ltd. (the "**Company**", "**we**", "**us**", "**our**") collects, uses, shares, transfers and retains personal data, and what rights you have in relation to that data.

1.2. It applies to you if you are a client, a prospective client, a visitor to our website or applications, an authorised representative or beneficial owner of a corporate client, an introducing broker, an affiliate, a supplier, a job applicant, or any other individual whose personal data we process.

1.3. This Policy forms part of our Legal Documentation and should be read together with our Terms and Conditions, Risk Disclosure, Order Execution Policy, Conflicts of Interest Policy and Cookie Policy.

1.4. A central point about this Policy. As a regulated financial services firm, a substantial part of the personal data we hold is held because the law requires us to hold it — for anti-money laundering and counter-terrorist financing purposes, for regulatory record-keeping, and for tax reporting. **Where that is the case, we cannot delete that data on request, and we cannot stop processing it, even if you close your account and ask us to.** Section 16 explains this in detail. We would rather state it clearly at the outset than bury it.

2. WHO WE ARE AND HOW TO CONTACT US

2.1. Data controller. [COMPANY LEGAL NAME], [ADDRESS], is the controller of the personal data described in this Policy.

2.2. Data Protection Officer. [Where a DPO is appointed:] Our Data Protection Officer can be contacted at [DPO EMAIL] or by post at the address above, marked for the attention of the Data Protection Officer. [Where no DPO is appointed: We have not appointed a Data Protection Officer as we are not required to do so. Privacy enquiries should be addressed to [PRIVACY EMAIL].]

2.3. EU / UK representative. [Where applicable, and required where the Company is established outside the EU/UK but offers services to individuals there:] Our representative for the purposes of [Article 27 GDPR / Article 27 UK GDPR] is [NAME], [ADDRESS], [EMAIL].

2.4. Joint controllers. [Where applicable:] In respect of [describe processing], we act as joint controller with [ENTITY]. The essence of our arrangement is available on request.

3. SCOPE

3.1. This Policy covers processing carried out through: our websites and landing pages; our client portal; our trading platforms and mobile applications; our onboarding and verification processes; our payment and withdrawal

processes; our client support, sales and retention channels; our marketing activity; and our dealings with introducing brokers, affiliates, suppliers and job applicants.

3.2. Our websites and platforms may contain links to, or embed content from, third parties. **We are not responsible for the privacy practices of any third party.** You should read the privacy notice of any third-party service you use, including any third-party trading platform, payment provider or social login provider.

4. PERSONAL DATA WE COLLECT

4.1. Identity data — full name, former names, date and place of birth, nationality, gender, national identification or passport number, tax identification number, photograph and image from identity documents, signature.

4.2. Contact data — residential address, correspondence address, email addresses, telephone numbers, and identifiers for messaging platforms where you contact us through them.

4.3. Verification and due diligence data — copies of identity documents, proof of address, selfie or liveness-check images where used, source of funds and source of wealth evidence, employment and occupation, bank and payment account details, beneficial ownership and control structure for corporate clients, politically exposed person status, sanctions and adverse media screening results, and the outcome of our risk assessment of you.

4.4. Financial and suitability data — declared income, net worth, savings and investments, investment objectives, risk tolerance, trading knowledge and experience, professional background, educational and professional qualifications, and your answers to our appropriateness questionnaire.

4.5. Account and transaction data — account numbers and types, base currency, leverage settings, balances and equity, deposits, withdrawals and internal transfers, payment method details, and the outcome of payment authorisations.

4.6. Trading data — orders placed, modified, cancelled, rejected and executed; instruments, volumes, prices, timestamps, slippage, commissions, spreads, swaps and adjustments; open and closed positions; margin levels, margin calls and stop-outs; use of expert advisors, copy trading and signal services.

4.7. Technical and device data — IP address, approximate location derived from IP address, device type and identifiers, operating system, browser type and version, screen resolution, language settings, time zone, login timestamps, session data, referring URLs, pages viewed, platform and application telemetry, and cookie and similar identifiers.

4.8. Communications data — the content and metadata of telephone calls, emails, live chats, in-platform messages, support tickets, video calls and messaging-app conversations with us; call recordings; and records of complaints.

4.9. Marketing and preference data — your marketing consents and objections, communication preferences, campaign and referral attribution data, and your responses to our communications.

4.10. Employment and recruitment data — where you apply to work with us: CV, references, qualifications, right-to-work documentation and background screening results.

4.11. We do not seek to collect data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, data concerning health, or data concerning sex life or sexual orientation. Where such data reaches us incidentally — for example, because it is visible on an identity document or is volunteered in a support conversation — we do not use it and we delete it where we lawfully can. Section 7 addresses the limited categories we do process.

5. WHERE WE OBTAIN YOUR PERSONAL DATA

5.1. Directly from you — through registration forms, the client portal, onboarding and verification, document uploads, questionnaires, deposits and withdrawals, trading activity, support conversations, complaints, surveys and events.

5.2. Automatically — through cookies and similar technologies, platform and application telemetry, and server logs.

5.3. From third parties, including:

- identity verification, document authentication and liveness-detection providers;
- sanctions, politically exposed person, adverse media and fraud-prevention databases;
- credit reference and address verification agencies, where used;
- payment service providers, acquirers, card schemes and banks;
- introducing brokers, affiliates, marketing partners and referral sources;
- money managers, strategy providers and third parties acting under a trading authority you have granted;
- public sources, including company registries, beneficial ownership registers, insolvency and litigation registers, regulatory registers and publicly available internet sources;
- our group companies, service providers and technology suppliers;
- regulators, tax authorities, law enforcement agencies and courts.

5.4. Where you provide us with personal data about another individual — for example a beneficial owner, an authorised representative, a joint account holder or a referee — **you must ensure you are entitled to do so** and must bring this Policy to their attention.

6. PURPOSES AND LAWFUL BASES FOR PROCESSING

6.1. We process personal data only where we have a lawful basis. Where we rely on legitimate interests, we have carried out a balancing assessment and you may request a summary of it.

Purpose	Data used	Lawful basis
Assessing and processing your application; opening and administering your account	Identity, contact, verification, financial	Performance of a contract, or steps at your request before entering into one; legal obligation
Identity verification, customer due diligence, ongoing monitoring, sanctions and PEP screening, suspicious activity detection and reporting	Identity, verification, transaction, trading, technical	**Legal obligation** under AML/CFT legislation; substantial public interest for special category data
Client categorisation and the appropriateness assessment	Financial, suitability	Legal obligation; performance of a contract
Executing your orders, maintaining your positions, calculating margin, applying swaps and adjustments	Account, transaction, trading	Performance of a contract
Processing deposits, withdrawals and payments; fraud and chargeback prevention	Account, transaction, technical	Performance of a contract; legal obligation; legitimate interests in preventing fraud and financial loss

Regulatory record-keeping, transaction reporting and communications recording	All categories	**Legal obligation** under financial services legislation
Tax reporting and withholding, including automatic exchange of information	Identity, account, transaction	Legal obligation
Client support, complaints handling and dispute resolution	All categories	Performance of a contract; legal obligation; legitimate interests in defending claims
Monitoring execution quality, slippage symmetry and platform performance	Trading, technical	Legitimate interests in meeting our best execution obligations and improving our service; legal obligation
Detecting and investigating abusive trading, market abuse, multi-account abuse and platform misuse	Trading, technical, account	Legal obligation; legitimate interests in protecting our business and other clients
Information security, access control, logging and business continuity	Technical, account, communications	Legitimate interests in securing our systems; legal obligation
Service communications about your account, our platforms and our terms	Contact, account	Performance of a contract; legal obligation
Marketing communications and personalisation	Contact, marketing, technical, trading	**Consent**, or legitimate interests where permitted for existing clients and subject to your right to object
Product development, analytics and business reporting	Aggregated and pseudonymised where possible	Legitimate interests in understanding and improving our services
Establishing, exercising or defending legal claims; corporate transactions	All categories	Legitimate interests; legal obligation
Recruitment	Employment	Steps prior to a contract; legitimate interests; legal obligation

6.2. Where a purpose relies on a legal obligation, you cannot object to that processing and we cannot stop it at your request, even if you close your account.

6.3. Segregation of AML data. Personal data collected and retained for anti-money laundering and counter-terrorist financing purposes is held for those purposes only. It is not used for marketing, and it is maintained separately from our commercial and marketing databases.

7. SPECIAL CATEGORY DATA AND CRIMINAL OFFENCE DATA

7.1. Biometric data. Where our onboarding process uses a selfie or liveness check compared against your identity document, the resulting facial template may constitute biometric data used for the purpose of uniquely identifying you, which is a special category of personal data. Where we process it, we do so on the basis of [substantial public interest in preventing and detecting money laundering, fraud and financial crime / your explicit consent], and we retain the biometric template only for as long as necessary to complete and evidence the verification.

7.2. Data revealing an alleged criminal offence. Sanctions screening, adverse media screening and politically exposed person screening may return information relating to criminal convictions, alleged offences or investigations. We process such data only where necessary to comply with our AML/CFT obligations and under the safeguards required by [Applicable Regulations], including restricted access and separate retention.

7.3. Health or vulnerability information. Where you tell us about a health condition, financial difficulty or other circumstance relevant to your treatment as a vulnerable client, we record only what is necessary to treat you appropriately, restrict access to it, and process it on the basis of [substantial public interest / your explicit consent].

7.4. We do not use special category data for marketing, profiling for commercial purposes, or automated decision-making other than as described at Section 8.

8. AUTOMATED DECISION-MAKING AND PROFILING

8.1. We use automated processing in the following ways.

8.2. Identity and document verification. Automated checks compare the identity document you upload against document templates and, where a liveness check is used, against your submitted image. A negative automated result does not by itself result in rejection: **it is referred for human review.**

8.3. Sanctions, PEP and adverse media screening. Automated screening generates alerts against watchlists and media sources. **All alerts are reviewed by a member of our Compliance team before any decision is taken.**

8.4. AML transaction monitoring and fraud detection. Automated rules and models flag unusual deposit, withdrawal and trading patterns. Flags are investigated by our Compliance team. Where a decision is taken to freeze, restrict or terminate an account, that decision is taken by a person.

8.5. Appropriateness assessment. Your answers to our questionnaire are scored automatically against defined criteria to determine whether trading CFDs is appropriate for you. **Where the outcome is negative, this results in a warning to you rather than an automatic refusal**, save where Applicable Regulations require otherwise. [Amend if the Company operates a hard block.]

8.6. Trading risk classification. We classify accounts internally for risk management purposes. **This classification does not affect the price you are quoted or the execution you receive** — see clause 6.5 of our Order Execution Policy. It informs how the Company manages its own market exposure.

8.7. Marketing segmentation. Where you have consented, we may segment audiences to determine which communications you receive. You may object at any time.

8.8. Your rights in relation to automated decisions. Where a decision producing legal effects concerning you, or similarly significantly affecting you, is based solely on automated processing, you have the right to obtain human intervention, to express your point of view and to contest the decision. Contact us at [PRIVACY EMAIL]. **We do not currently take any decision of that kind without human involvement**, with the exception of automated risk-control functions in the trading platform (such as the automatic stop-out described in our Terms and Conditions), which operate on account-level values rather than on a profile of you as an individual.

9. MARKETING COMMUNICATIONS

9.1. We send marketing communications by email, SMS, telephone, push notification and post where you have consented, or where we are permitted to do so on the basis of an existing client relationship in respect of similar products and services.

9.2. You can withdraw consent or object at any time, using the unsubscribe link in any electronic message, through the preferences section of your client portal, or by contacting [PRIVACY EMAIL]. Withdrawal takes effect for the future and does not affect the lawfulness of processing carried out before it.

9.3. Withdrawing marketing consent does not stop service communications — messages about your account, margin, changes to our terms, platform maintenance, corporate actions and regulatory notices. We are required to send those.

9.4. Retention and vulnerability. We apply internal restrictions on contacting clients who have sustained significant losses, who have requested a withdrawal, or who have indicated financial difficulty. These restrictions are described in our Conflicts of Interest Policy.

9.5. Where an introducing broker, affiliate or marketing partner contacts you, they do so as controller of the data they hold about you and under their own privacy notice. **We require our partners to comply with applicable marketing rules, but we are not responsible for communications they send without our authority.** Please report any such communication to [COMPLIANCE EMAIL].

10. COOKIES AND SIMILAR TECHNOLOGIES

10.1. We use cookies, pixels, SDKs, local storage and similar technologies on our websites and applications for: strictly necessary purposes (session management, security, load balancing, fraud prevention); functionality (language, layout and platform preferences); analytics (understanding how our services are used); and advertising and attribution (measuring campaign performance and, where you consent, delivering targeted advertising).

10.2. Strictly necessary cookies are set without consent. All other categories are set only where you consent, and you may withdraw consent at any time through our cookie banner or preference centre.

10.3. Full details of the cookies used, their purposes, providers and durations are set out in our Cookie Policy at [URL].

10.4. Some analytics and advertising technologies are provided by third parties who may act as independent controllers of the data they collect. Their processing is governed by their own privacy notices.

11. RECORDING OF TELEPHONE CALLS AND ELECTRONIC COMMUNICATIONS

11.1. We record telephone conversations and electronic communications relating to the reception, transmission and execution of orders, and those intended to result in a transaction, whether or not a transaction ultimately results.

11.2. We do this because financial services legislation requires it. Under the MiFID II framework, for example, the obligation to record such communications is imposed by Article 16(7) of Directive 2014/65/EU, with the technical requirements — durable medium, tamper-evidence, traceability of access and accessibility to the regulator — set out in Article 76 of Commission Delegated Regulation (EU) 2017/565. **The records must be kept for a minimum of five years and, where the competent authority requests it, for up to seven years.** For UK firms the equivalent rules are onshored in the FCA Handbook at SYSC 10A.

11.3. You have the right to a copy of a recording of your own conversations and communications with us on request, for the applicable retention period. Contact [PRIVACY EMAIL]. We may need to verify your identity and may redact information relating to other individuals.

11.4. Recordings are stored so that they cannot be altered, deleted or overwritten after capture, and every access to them is logged.

11.5. We may also record or monitor communications not covered by clause 11.1 — for example general support calls and chats — for quality assurance, training, security and complaint-handling purposes, on the basis of our legitimate interests.

11.6. Do not use unmonitored channels for order instructions. We may be unable to act on, or to evidence, instructions sent through channels we are not permitted to record.

12. WHO WE SHARE YOUR PERSONAL DATA WITH

12.1. We share personal data with the categories of recipient set out at Annex II, which include: our group companies; identity verification and screening providers; payment service providers and banks; liquidity providers and technology suppliers (including trading platform, hosting, CRM, communications-recording and analytics providers); professional advisers, auditors and insurers; introducing brokers, affiliates and money managers, where relevant to your relationship with them; debt recovery agents; regulators, tax authorities, financial intelligence units, law enforcement agencies and courts; and, in the event of a corporate transaction, prospective buyers and their advisers.

12.2. Where a recipient processes personal data on our instructions, it acts as our processor and is bound by a written agreement imposing confidentiality, security and sub-processing controls.

12.3. Where a recipient determines its own purposes — for example a payment provider, an introducing broker, or a regulator — it acts as an independent controller and its own privacy notice applies.

12.4. We do not sell personal data.

12.5. We disclose personal data to authorities where we are legally required to do so. **Where a disclosure relates to a suspicion of money laundering or terrorist financing, we are prohibited by law from informing you of it.** See Section 16.

13. INTERNATIONAL TRANSFERS

13.1. Some of our group companies, service providers and infrastructure are located outside [the European Economic Area / the United Kingdom / your country of residence]. Where personal data is transferred to such a country, we ensure an appropriate transfer mechanism is in place, being one of:

- **(a)** an adequacy decision by the relevant authority in respect of the destination country or framework;
- **(b)** Standard Contractual Clauses approved by the European Commission or, for UK transfers, the UK International Data Transfer Agreement or Addendum, supplemented where necessary by a transfer impact assessment and additional technical and organisational measures;
- **(c)** Binding Corporate Rules, where applicable;
- **(d)** a derogation permitted by Applicable Regulations, used only where no other mechanism is available.

13.2. Transfers to the United States. Where we transfer personal data to a recipient in the United States, we rely on the EU–US Data Privacy Framework where the recipient is certified under it, and otherwise on Standard Contractual Clauses.

13.3. Status of the EU–US Data Privacy Framework. The Framework was adopted by the European Commission on 10 July 2023 as an adequacy decision under Article 45 GDPR. It was challenged before the General Court of the European Union, which dismissed that challenge on 3 September 2025 and upheld the Framework; an appeal to the Court of Justice of the European Union was lodged in October 2025 and remains pending. **The**

Framework therefore remains valid law, but its long-term status is subject to that pending litigation. We monitor its status and maintain Standard Contractual Clauses as a fallback mechanism for transfers currently relying on it, so that transfers can continue lawfully if the position changes.

13.4. You may request a copy of the safeguards applied to a particular transfer by contacting [PRIVACY EMAIL]. We may redact commercially confidential terms.

14. HOW LONG WE KEEP YOUR PERSONAL DATA

14.1. We keep personal data only for as long as necessary for the purposes for which it was collected, and for as long as we are required to keep it by law. A summary schedule is at Annex I.

14.2. AML and customer due diligence records. These are retained for at least **five years from the end of the business relationship** or from the date of an occasional transaction. Some jurisdictions require longer — for example, the Netherlands and France apply a minimum of five years, while Spain and Luxembourg apply ten. From **10 July 2027**, Regulation (EU) 2024/1624 (the EU Anti-Money Laundering Regulation) replaces divergent national rules with a single harmonised retention standard, and where legal proceedings relating to suspected money laundering or terrorist financing are pending on that date, relevant information may be retained for five years from it, with Member States able to allow or require a further five years subject to necessity and proportionality. [Confirm the period applicable in the Company's jurisdiction and update this clause.]

14.3. Recorded communications. Retained for a minimum of five years from the date of the recording — not from the date of any resulting transaction — and for up to seven years where the competent authority requests it. Where we operate in a jurisdiction whose authority routinely exercises that option, we retain for seven years by default.

14.4. Transaction and order records. Retained for the period required by financial services legislation, being at least five years.

14.5. Tax records. Retained for the period required by applicable tax law.

14.6. Litigation hold. Where personal data is relevant to actual or anticipated legal proceedings, a regulatory investigation or a complaint, it is retained until the matter is concluded and any appeal period has expired, even where a retention period would otherwise have expired.

14.7. Marketing data. Retained until you withdraw consent or object, and thereafter only the minimum record needed to honour your objection — that is, we keep enough information to ensure we do not contact you again.

14.8. Prospective clients who do not complete onboarding. Retained for [XX] months, save where AML obligations require longer retention of verification data already collected.

14.9. Technical and log data. Retained for [XX] months for security and fraud prevention purposes, longer where relevant to an investigation.

14.10. At the end of the applicable period, personal data is securely deleted or irreversibly anonymised. **Deletion is applied automatically on expiry of the retention period**, rather than only on request.

15. YOUR RIGHTS

15.1. Subject to Section 16, you have the following rights.

15.2. Access — to be told whether we process personal data about you and, if so, to receive a copy of it together with information about how it is used.

15.3. Rectification — to have inaccurate personal data corrected and incomplete data completed.

15.4. Erasure — to have personal data deleted where it is no longer necessary, where you withdraw consent and no other basis applies, or where it has been processed unlawfully.

15.5. Restriction — to have processing limited in defined circumstances, for example while the accuracy of data is being verified.

15.6. Portability — to receive personal data you provided to us in a structured, commonly used, machine-readable format, and to have it transmitted to another controller where technically feasible. This applies to data processed on the basis of consent or contract by automated means.

15.7. Objection — to object to processing based on our legitimate interests, on grounds relating to your particular situation, and to object at any time and without qualification to processing for direct marketing.

15.8. Withdrawal of consent — at any time, where processing is based on consent.

15.9. Human intervention in automated decisions — as described at clause 8.8.

15.10. Complaint — to lodge a complaint with a supervisory authority (Section 21).

15.11. How to exercise your rights. Contact [PRIVACY EMAIL]. We will respond within one month, extendable by two further months for complex or numerous requests, in which case we will tell you within the first month. We will verify your identity before disclosing personal data. Exercising your rights is free of charge, unless a request is manifestly unfounded or excessive, in which case we may charge a reasonable fee or refuse to act and will explain why.

16. LIMITS ON YOUR RIGHTS

16.1. This Section is important and we ask you to read it. Data protection rights are not absolute, and in a regulated financial services context several of them are materially restricted.

16.2. Erasure. We cannot delete personal data we are required by law to retain — in particular AML and customer due diligence records, recorded communications, order and transaction records, and tax records. **Closing your account does not trigger deletion of that data.** It triggers the start of the applicable statutory retention period.

16.3. Objection and restriction. You cannot object to, or restrict, processing carried out to comply with a legal obligation.

16.4. Portability. This right does not extend to data we generate about you (such as our risk assessment of you) or to data processed on the basis of a legal obligation.

16.5. Tipping off. Where we have made, or are considering making, a report of suspected money laundering or terrorist financing, we are prohibited by law from telling you. In those circumstances we may be required to **decline to confirm or deny** whether we hold particular data, to refuse a subject access request in whole or in part, and to give no substantive reason. Article 23 GDPR expressly permits Member States to restrict data subject rights on these grounds, and the tipping-off prohibition overrides the transparency obligations that would otherwise apply. **A restricted response of this kind is not evidence that a report has been made, and should not be read as such.**

16.6. Other restrictions. We may also restrict a response where it would: prejudice the prevention, detection or investigation of crime; prejudice a regulatory function; disclose the personal data of another individual who has not consented; disclose legally privileged material; or prejudice the establishment, exercise or defence of legal claims.

16.7. Where we restrict a response, we record the decision and the reasoning, and we tell you as much as we lawfully can — including, where permitted, that you may complain to the supervisory authority.

17. SECURITY

17.1. We maintain technical and organisational measures appropriate to the risk, including: encryption of data in transit and at rest; access control on a least-privilege basis; multi-factor authentication for administrative access; network segmentation and monitoring; logging of access to client records and to communications recordings; vulnerability management and penetration testing; secure development practices; supplier due diligence and contractual security obligations; staff training and confidentiality obligations; and backup, business continuity and disaster recovery arrangements, including geographically separated and regularly tested backups of recorded communications.

17.2. What we ask of you. Keep your credentials confidential, use a unique password and enable multi-factor authentication. **We will never ask you for your password or for a one-time code.** Notify us immediately at [SECURITY EMAIL] if you suspect unauthorised access.

17.3. No transmission over the internet is entirely secure. Information sent by unencrypted email may be intercepted. Where you send us sensitive documents, use the secure upload facility in your client portal rather than email.

18. PERSONAL DATA BREACHES

18.1. We maintain an incident response procedure covering detection, containment, assessment, notification and remediation.

18.2. Where a breach is likely to result in a risk to the rights and freedoms of individuals, we notify the competent supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of it.

18.3. Where a breach is likely to result in a **high** risk to you, we will notify you without undue delay and describe what happened, the likely consequences, the measures we have taken, and what you should do.

18.4. We maintain an internal register of all personal data breaches, whether or not notifiable.

19. CHILDREN

19.1. Our services are not available to persons under 18, or under the age of majority in their jurisdiction if higher. We do not knowingly collect personal data from children.

19.2. If we become aware that we hold personal data of a child, we will delete it, save where a legal obligation requires retention.

20. CHANGES TO THIS POLICY

20.1. We may amend this Policy from time to time. The current version is always available at [URL].

20.2. Where a change is material — for example a new purpose, a new category of recipient, a change of lawful basis, or a significant change to retention — we will notify you in advance by email or through the client portal.

20.3. We maintain all previous versions of this Policy and can provide the version applicable at any given date on request.

21. COMPLAINTS AND SUPERVISORY AUTHORITIES

21.1. If you are concerned about how we handle your personal data, please contact us first at [PRIVACY EMAIL] so that we have the opportunity to put things right.

21.2. You also have the right to lodge a complaint with a supervisory authority — in the Member State of your habitual residence, your place of work, or the place of the alleged infringement.

- **Our lead supervisory authority:** [AUTHORITY NAME], [ADDRESS], [WEBSITE], [PHONE]
- **[Where applicable] United Kingdom:** Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, ico.org.uk

21.3. Complaints about our financial services conduct — as opposed to our data handling — should be made under our Complaints Handling Policy at [URL].

- **Privacy enquiries:** [PRIVACY EMAIL]
- **Data Protection Officer:** [DPO EMAIL]
- **Security incidents:** [SECURITY EMAIL]
- **Address:** [REGISTERED ADDRESS]

Document control

Owner	[Data Protection Officer / Compliance Department]
Version	1.0
Approved by	[Board of Directors], [DATE]
Next review	[DATE] — at least annually
Related documents	Terms and Conditions; Risk Disclosure; Order Execution Policy; Conflicts of Interest Policy; Cookie Policy; Complaints Handling Policy; Record of Processing Activities; Data Retention Schedule; Incident Response Procedure

ANNEX I — RETENTION SCHEDULE

Summary only. The Company maintains a full internal retention schedule. Verify each period against the law of the Company's jurisdiction before publication.

Category	Retention period	Basis

Customer due diligence and KYC records	Minimum 5 years from end of relationship; longer where national law requires (up to 10 in some Member States)	AML/CFT legislation
Sanctions, PEP and adverse media screening results	As above	AML/CFT legislation
Suspicious activity reports and supporting material	As required by the financial intelligence unit; not less than 5 years	AML/CFT legislation
Recorded telephone calls and electronic communications relating to orders	Minimum 5 years from date of recording; up to 7 where the competent authority requests	Financial services legislation
Order, transaction and execution records	Minimum 5 years	Financial services legislation
Client agreements and disclosures provided	Duration of relationship plus [5] years	Contract; legal obligation
Complaints records	[5] years from closure	Legal obligation; defence of claims
Appropriateness assessment records	Duration of relationship plus [5] years	Legal obligation
Tax reporting records	As required by applicable tax law	Legal obligation
Marketing consents and objections	Until withdrawn, then minimum suppression record indefinitely	Consent; legitimate interests
Incomplete applications	[XX] months	Legitimate interests
Website and platform technical logs	[XX] months	Legitimate interests; security
Recruitment records (unsuccessful)	[XX] months	Legitimate interests; consent
Any data subject to litigation hold	Until conclusion of the matter and expiry of appeal periods	Defence of legal claims

ANNEX II — CATEGORIES OF RECIPIENTS

Category	Role	Typical purpose
Group companies	Controller / processor	Shared services, risk management, support
Identity verification and screening providers	Processor	KYC, document authentication, liveness, sanctions and PEP screening
Payment service providers, acquirers and banks	Independent controller	Deposits, withdrawals, fraud prevention
Trading platform and technology providers	Processor	Platform operation, hosting, connectivity
Communications recording and archiving providers	Processor	Regulatory call and message retention
CRM, marketing and analytics providers	Processor / independent controller	Client management, campaign delivery, analytics
Liquidity providers	Independent controller	Hedging of the Company's own exposure (no client identity disclosed)

Introducing brokers, affiliates and money managers	Independent controller	Client introduction and, where authorised, account management
Professional advisers, auditors and insurers	Independent controller / processor	Legal, audit, insurance
Regulators, tax authorities, FIUs, law enforcement, courts	Independent controller	Legal and regulatory obligations
Debt recovery and litigation support	Processor / independent controller	Recovery of sums due; legal proceedings
Prospective purchasers in a corporate transaction	Independent controller	Due diligence, subject to confidentiality

APPENDIX — DRAFTING NOTES

Remove this appendix before publication. It is guidance for you and your legal counsel, not client-facing content.

A. The structural problem this document has to solve

A CFD broker's privacy policy is not really a privacy policy. It is a document about the collision between two bodies of law that pull in opposite directions. GDPR demands data minimisation, storage limitation, purpose limitation and transparency. AML law demands extensive collection, multi-year retention, surveillance of transactions, and reporting about clients **without telling them**. The resolution that regulators expect is: Article 6(1)(c) as the lawful basis for AML processing, Article 23 restrictions on data subject rights where tipping-off is a risk, and clear segregation of AML data from marketing and commercial processing.

Most broker privacy policies are generic e-commerce templates with "KYC" pasted in. That is the wrong shape entirely. This draft is built around the collision — which is why Section 16 (Limits on Your Rights) exists as a full section rather than a sentence, and why clause 6.3 and clause 1.4 exist at all.

B. Retention — the numbers you must verify, not assume

These are the three periods that get brokers into trouble, and they are all jurisdiction-sensitive:

1. **AML records: 5 years from end of relationship** is the floor. National law diverges — the Netherlands and France apply five years, Spain and Luxembourg ten. **This divergence disappears on 10 July 2027**, when Regulation (EU) 2024/1624 (AMLR) applies directly in all 27 Member States with no national transposition layer, replacing the fragmented AMLD-based regime. Article 77 AMLR is the harmonised retention provision. AMLA, the new EU supervisor in Frankfurt, has been operational since 1 July 2025 and takes up direct supervision from 2028. If you are going EU-regulated, clause 14.2 must be revisited before that date.
2. **Call recordings: 5 years minimum, 7 on request.** Article 16(7) MiFID II, with technical detail in Article 76 of Delegated Regulation (EU) 2017/565. **The clock starts at the date of recording, not the date of any resulting transaction** — a detail many firms get wrong in their retention configuration. Some authorities routinely exercise the seven-year option; where yours does, set seven as the default. UK equivalent is SYSC 10A.
3. **Litigation hold overrides everything.** Clause 14.6.

Also note clause 14.10 — automated deletion on expiry, not deletion on request. That is the specific configuration regulators look for, and it is an engineering commitment, not a drafting one.

C. International transfers — say something true about the DPF, not a boilerplate line

Clause 13.3 states the actual position: the Framework was adopted July 2023, the General Court dismissed the Latombe challenge on 3 September 2025 and upheld it, and an appeal to the CJEU was lodged in October 2025 and is pending. Commentators refer to the prospective successor challenge as "Schrems III"; both predecessor frameworks (Safe Harbor and Privacy Shield) were struck down by the CJEU. Two of the underlying US safeguards have been weakened since early 2025, including the loss of quorum at the Privacy and Civil Liberties Oversight Board.

The practical consequence for you is clause 13.3's last sentence: **keep SCCs in place as a fallback for every US transfer currently relying on the DPF.** If the CJEU annuls the adequacy decision, firms with no fallback have to suspend transfers overnight. Firms with SCCs already executed keep operating. This costs nothing to do now.

D. What is coming that this Policy does not yet reflect

The European Commission published the **Digital Omnibus** package on 19 November 2025, proposing amendments to GDPR, ePrivacy, NIS2, DORA and the AI Act — including a narrower, more "relative" definition of personal data, an explicit legitimate-interest basis for AI development, new Article 9 exceptions, and an overhaul of the cookie consent rules. **It is not law.** The AI half moved faster (Council adoption 29 June 2026); the data half covering GDPR and ePrivacy remains under negotiation, with final adoption not expected before late 2026 at the earliest, and the Council's working text omitting several core consent provisions. Do not draft to it. But if the cookie provisions land, Section 10 and your Cookie Policy will need revisiting.

E. Clauses that commit you to an operational reality

- **6.3 / 14.10** — AML data segregated from marketing databases, and automated deletion at expiry. Both are database architecture, not policy text.
- **8.2–8.4** — human review of every screening alert and every negative verification result. If your onboarding auto-rejects, clause 8.2 is false as written.
- **8.6** — the internal risk classification does not affect pricing or execution. This is the same representation as clause 6.5 of the Order Execution Policy and Section 7.2 of the Conflicts of Interest Policy. Three documents, one factual claim. It has to be true.
- **11.4** — tamper-evident storage with logged access. Standard file servers and off-the-shelf video conferencing recordings generally do not satisfy this.
- **16.5** — your Compliance team needs a documented procedure and decision log for restricted DSAR responses, and the people answering DSARs need to know not to improvise.

F. Documents you need behind this one

This Policy is the client-facing surface of a compliance framework. It presupposes you also hold, internally: a Record of Processing Activities (ROPA) documenting Article 6(1)(c) as the basis for all KYC and transaction monitoring; a full data retention schedule citing the specific legal article for each period; data processing agreements with every processor; executed SCCs; transfer impact assessments; a DPIA for the biometric liveness check and for the transaction monitoring models; and a documented legitimate interests assessment for each purpose in the table at 6.1 where that basis is claimed. **A regulator that asks for these and receives only this Policy will treat the Policy as unsupported.**

G. Legal review

I am not a lawyer and this is not legal advice. Data protection is more jurisdiction-specific than the other documents in this set, and several clauses above are placeholders for national law that I cannot resolve without knowing your regulator. This requires review by counsel qualified in your jurisdiction and, ideally, by a data protection specialist.