

PRIVACY POLICY

1. INTRODUCTION

- 1.1. Flare FX (Pty) Ltd, registration number 2023/202257/07, trading as “FlareX” (“FlareX”, “we”, “us” or “our”), is a private company duly incorporated in accordance with the laws of the Republic of South Africa.
- 1.2. FlareX conducts regulated financial markets and financial services activities in South Africa pursuant to two distinct regulatory authorisations.
- 1.3. FlareX is:
 - 1.3.1. an authorised Over-the-Counter Derivative Provider (“ODP”), ODP No. 83, under the South African regulatory framework governing over-the-counter derivatives; and
 - 1.3.2. an authorised Category I Financial Services Provider (“FSP”) and Crypto Asset Service Provider (“CASP”) in terms of the Financial Advisory and Intermediary Services Act 37 of 2002 (“FAIS”), under FSP No. 54894.
- 1.4. Where FlareX provides any other regulated services, the processing of personal information associated with those services is also governed by this Policy, subject to the applicable legal and regulatory requirements.

2. PURPOSE AND COMMITMENT

- 2.1. FlareX FX respects the privacy of individuals and juristic persons whose personal information it processes. This Privacy Policy explains, in clear terms, what personal information we collect, why we collect it, how we use and protect it, when we disclose it, how long we retain it, when information may leave South Africa, and how a data subject may exercise rights under POPIA.
- 2.2. This Policy is intended to satisfy the transparency and notification requirements of POPIA and should be read together with FlareX’s agreements, notices, PAIA Manual, records-retention arrangements and other applicable policies.

3. SCOPE

- 3.1. This Policy applies to personal information processed by FlareX in connection with its business and services, including information relating to clients, prospective clients, authorised representatives, beneficial owners, directors and officers, employees, applicants, introducers and business partners, service providers, website users and other persons whose information FlareX lawfully receives.
- 3.2. It applies to information collected electronically, in paper records, through telephone or other communications, through FlareX’s website or platforms, and from third parties or public and regulatory sources.

4. DEFINITIONS

Term	Meaning
“Data subject”	the person to whom personal information relates. Depending on the circumstances, this may include a natural person or a juristic person.
“Personal information”	information relating to an identifiable, living natural person and, where applicable, an identifiable existing juristic person, including information such as identification, contact, financial, employment and transaction information.
“POPI Act”	means the Protection of Personal Information Act, No. 4 of 2013, as amended;
“Processing”	any operation or activity concerning personal information, including collection, recording, organisation, storage, updating, retrieval, use, disclosure, transfer, restriction, destruction or deletion.
“Responsible party”	FlareX, where it determines the purpose of and means for processing personal information.
“Operator”	a person or entity that processes personal information for a responsible party in terms of a mandate, without coming under the direct authority of that responsible party.
“Special personal information”	categories of information regulated more strictly by POPIA, including information concerning race or ethnic origin, political persuasion, religious or philosophical beliefs, trade-union membership, health or sex life, biometric information and certain criminal-behaviour information.
“Information Officer”	the person designated by FlareX to perform the functions required under POPIA and PAIA.

“Information Regulator”	the Information Regulator established under POPIA and responsible for, among other things, administering POPIA and PAIA.
--------------------------------	--

5. POPIA PRINCIPLES AND OUR RESPONSIBILITIES

- 5.1. FlareX is accountable for ensuring that personal information is processed in accordance with POPIA. In particular, we apply the eight conditions for lawful processing by ensuring that personal information is processed responsibly, lawfully and reasonably; collected for specific, explicitly defined and lawful purposes; limited to information that is adequate, relevant and not excessive; kept accurate and up to date where reasonably practicable; handled transparently; protected by appropriate security safeguards; and subject to data-subject participation rights.
- 5.2. FlareX will maintain appropriate internal governance, policies, procedures, controls and training to support compliance. Where processing is outsourced, FlareX will use appropriate contractual and operational safeguards and require operators to maintain confidentiality and security measures appropriate to the nature of the information.

6. PERSONAL INFORMATION WE MAY COLLECT

- 6.1. The information collected depends on the relationship with FlareX and the service or transaction involved. It may include:
- 6.1.1. Identification and verification information, including names, identity or passport details, nationality, date of birth, residential address, proof of address and verification results;
 - 6.1.2. Contact information, including telephone numbers, email addresses, postal and physical addresses and communication preferences;
 - 6.1.3. Financial and transactional information, including bank-account details, payment information, source-of-funds and source-of-wealth information where required, transaction history, deposits, withdrawals and related records;
 - 6.1.4. Employment, business and professional information, including employer, occupation, company details, directorships, ownership information and beneficial ownership information;
 - 6.1.5. Regulatory, compliance and risk information, including Client Due Diligence information, sanctions and screening results, risk assessments, fraud indicators, complaints, regulatory correspondence and information required to meet legal obligations;
 - 6.1.6. Trading and platform information, including account identifiers, trading activity, orders, positions, device information, IP address, login information and records of communications with FlareX;
 - 6.1.7. Information contained in communications and supporting documents provided to FlareX, including correspondence, call records where lawfully recorded, forms, applications and contractual documents

- 6.1.8. Information obtained from third parties, including banks, payment providers, introducers, group entities, professional advisers, credit or verification providers, public sources, regulatory authorities and law-enforcement or government bodies, where lawfully permitted; and
- 6.1.9. Special personal information or children's information only where permitted by POPIA and other applicable law, and where a lawful basis and appropriate safeguards exist.

7. HOW WE COLLECT PERSONAL INFORMATION

- 7.1. FlareX may collect personal information directly from the data subject, from authorised representatives, through its website or platforms, through forms and agreements, during communications with the data subject, or from third parties where lawful and reasonably necessary for a legitimate business or regulatory purpose.
- 7.2. Where information is collected directly from a data subject, FlareX will, as required by POPIA, take reasonable steps to make the data subject aware of the information being collected, the purpose of collection, whether provision is voluntary or mandatory, the consequences of failing to provide it, and relevant legal or regulatory requirements. Where information is obtained from another source, FlareX will apply the requirements and exceptions applicable to indirect collection under POPIA.

8. PURPOSES FOR WHICH WE PROCESS PERSONAL INFORMATION

- 8.1. FlareX processes personal information only for a specific, explicitly defined and lawful purpose related to its functions and activities. Depending on the relationship and applicable law, purposes may include:
 - 8.1.1. establishing, verifying and maintaining client and counterparty relationships;
 - 8.1.2. Client due diligence, enhanced due diligence, sanctions screening, transaction monitoring, fraud prevention and financial-crime controls;
 - 8.1.3. complying with POPIA, FIC Act, Financial Markets Act, FSCA requirements, tax requirements and other applicable laws, regulations, directives, standards and lawful regulatory requests;
 - 8.1.4. providing, administering and supporting FlareX's products, services, trading accounts and platforms;
 - 8.1.5. processing deposits, withdrawals, payments, settlements and related reconciliations;
 - 8.1.6. assessing and managing operational, credit, market, liquidity, fraud, financial-crime and other risks;
 - 8.1.7. communicating with data subjects about accounts, transactions, services, security matters, regulatory requirements, complaints and support requests;
 - 8.1.8. investigating and managing complaints, disputes, incidents and suspected misconduct;
 - 8.1.9. maintaining accounting, audit, legal, governance and business records;
 - 8.1.10. protecting FlareX, its clients, personnel, systems and assets against fraud, cyber threats, abuse and other unlawful activity;
 - 8.1.11. improving systems, controls, service delivery and operational processes, where permitted by law; and

- 8.1.12. marketing FlareX's own services where the requirements for direct marketing under POPIA have been met.

9. LAWFUL GROUNDS FOR PROCESSING

- 9.1. POPIA does not permit FlareX to process personal information merely because the information is useful or commercially convenient. Processing must be justified under the applicable provisions of POPIA. Depending on the circumstances, FlareX may rely on one or more of the following grounds:
- 9.1.1. Consent given by the data subject, where consent is required and is appropriate as the lawful ground.
 - 9.1.2. Necessity for taking steps at the request of the data subject before entering into a contract or for performing a contract to which the data subject is party.
 - 9.1.3. Compliance with an obligation imposed by law, regulation, license condition or other applicable legal requirement.
 - 9.1.4. Protection of a legitimate interest of the data subject in circumstances permitted by POPIA.
 - 9.1.5. Performance of a public-law duty by a public body, where applicable.
 - 9.1.6. Pursuit of the legitimate interests of FlareX or a third party to whom the information is supplied, where permitted by POPIA and where the processing is not unjustified in the circumstances.
- 9.2. Where consent is relied upon, it will be requested in a manner that is voluntary, specific and informed, and the data subject may withdraw consent. Withdrawal of consent does not invalidate processing that was lawful before withdrawal, and withdrawal will not necessarily result in deletion where FlareX is legally required or otherwise permitted to retain the information.

10. SPECIAL PERSONAL INFORMATION AND CHILDREN

- 10.1. FlareX recognises that POPIA imposes additional restrictions on special personal information and personal information relating to children. FlareX will not process special personal information or children's information unless a lawful exception or authorisation applies, and the processing is necessary and proportionate to the relevant purpose.
- 10.2. Where special personal information is encountered as part of Client Due Diligence, AML, fraud, employment, regulatory or other processes, FlareX will apply enhanced access, security, retention and governance controls appropriate to the information. FlareX will not knowingly collect or process a child's personal information for ordinary client onboarding unless the processing is permitted by POPIA and appropriate safeguards are in place.

11. INFORMATION QUALITY, MINIMIZATION AND PURPOSE LIMITATION

- 11.1. FlareX will take reasonably practicable steps to ensure that personal information is complete, accurate, not misleading and updated where necessary, having regard to the purpose for which it is collected or further processed. FlareX will seek to collect information that is adequate, relevant and not excessive for the

relevant purpose and will avoid using personal information for incompatible purposes unless POPIA permits further processing.

- 11.2. Data subjects should promptly notify FlareX if information supplied to FlareX is inaccurate, incomplete or out of date.

12. SHARING AND DISCLOSURE OF PERSONAL INFORMATION

- 12.1. FlareX may disclose personal information where necessary and lawful, including to:
- 12.1.1. the FSCA and other regulators, supervisory bodies and statutory authorities;
 - 12.1.2. the Financial Intelligence Centre, South African Revenue Service, law-enforcement agencies, courts and other competent authorities where required or permitted by law;
 - 12.1.3. banks, payment service providers, custodians, liquidity or execution counterparties and other transaction-service providers where necessary to provide the relevant service;
 - 12.1.4. technology, hosting, cybersecurity, verification, screening, communications, document-management, audit, legal, accounting and other service providers acting as operators or independent responsible parties, as applicable;
 - 12.1.5. professional advisers and auditors where necessary for legitimate business, legal, governance or regulatory purposes;
 - 12.1.6. FlareX group entities, where applicable, subject to lawful purpose, confidentiality and security requirements; and,
 - 12.1.7. other persons where the disclosure is authorised by the data subject or otherwise permitted by law.
- 12.2. FlareX will not sell personal information as a general commercial practice. Where an operator processes information on FlareX's behalf, FlareX will require appropriate confidentiality and security measures and will take reasonable steps to ensure compliance with POPIA.

13. OPERATORS AND THIRD-PARTY PROCESSORS

- 13.1. Where FlareX appoints an operator to process personal information on its behalf, FlareX will enter into appropriate written arrangements requiring the operator to process information only with FlareX's authorisation, keep the information confidential, implement appropriate security safeguards, notify FlareX of security compromises without undue delay, and comply with applicable data-protection requirements.
- 13.2. Where a third party determines its own purposes and means of processing, that party may be a separate responsible party rather than an operator. FlareX will assess the relationship and apply appropriate contractual and governance arrangements accordingly.

14. INFORMATION SECURITY

- 14.1. FlareX takes appropriate, reasonable technical and organisational measures to protect personal information against loss, damage, unauthorised destruction, unlawful access, unauthorised processing and other foreseeable risks. Measures may include:
- 14.1.1. access controls based on business need and appropriate authorisation;
 - 14.1.2. authentication, password and privileged-access controls;
 - 14.1.3. encryption or other appropriate protection of information in transit and/or at rest, where appropriate;
 - 14.1.4. network, endpoint, application and infrastructure security controls;
 - 14.1.5. logging, monitoring, incident detection and response measures;
 - 14.1.6. backup, recovery and business-continuity arrangements;
 - 14.1.7. security testing, assessments and reviews appropriate to the risks;
 - 14.1.8. employee confidentiality obligations, awareness and training;
 - 14.1.9. secure disposal and destruction of information when retention is no longer required; and,
 - 14.1.10. security and confidentiality requirements imposed on relevant operators and service providers.
- 14.2. No method of transmission or storage can be guaranteed to be completely secure. FlareX will nevertheless continually assess and improve safeguards in response to changes in technology, threats, operational risks and identified deficiencies.

15. PERSONAL INFORMATION SECURITY COMPROMISES

- 15.1. If FlareX has reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, FlareX will assess and manage the incident under its incident-response procedures and POPIA. Where section 22 of POPIA applies, FlareX will notify the Information Regulator and the affected data subject(s) as soon as reasonably possible after discovery of the compromise.
- 15.2. A notification may include the nature of the compromise, the personal information reasonably believed to have been accessed or acquired, the identity of the unauthorised person where known, the measures taken or proposed to address the compromise, and measures recommended to data subjects to mitigate possible adverse consequences.

16. CROSS-BORDER TRANSFERS

- 16.1. Personal information may be processed or stored outside South Africa where FlareX uses international service providers, group entities or other service arrangements. FlareX will only transfer personal information across borders in circumstances permitted by section 72 of POPIA, including where the recipient is subject to an adequate level of protection, the relevant data subject has consented after being informed of the transfer where consent is relied upon, the transfer is necessary for a contract, or another statutory exception applies.

- 16.2. Where appropriate, FlareX will use contractual, technical and organisational safeguards to protect information transferred outside South Africa. Data subjects may contact the Information Officer for information about material categories of international recipients relevant to their relationship with FlareX.

17. DIRECT MARKETING

- 17.1. FlareX will comply with POPIA requirements applicable to direct marketing. Electronic direct marketing, including marketing by email, SMS, messaging applications or other electronic communications, will only be undertaken where a lawful basis under section 69 applies.
- 17.2. Where consent is required, FlareX will obtain it in an accessible manner and will provide a simple and free opportunity to withdraw or object. Where FlareX relies on the existing-customer exception in section 69, it will limit marketing to its own similar products or services and provide the required opportunity to object at the time information is collected and in each marketing communication.
- 17.3. A data subject may opt out of marketing at any time by using the unsubscribe mechanism provided or contacting the Information Officer. An opt-out from marketing does not prevent FlareX from sending service, security, contractual, regulatory or other non-marketing communications that FlareX is required or permitted to send.

18. COOKIES, WEBSITE AND ELECTRONIC IDENTIFIERS

- 18.1. FlareX's website and digital platforms may use cookies, device identifiers, log files, IP addresses and similar technologies for security, functionality, analytics, performance and, where applicable, marketing. Where these technologies involve personal information, FlareX will process the information in accordance with POPIA and any applicable cookie notice or consent mechanism.
- 18.2. Users can manage certain cookie settings through their browser or device. Disabling certain cookies may affect the functionality or security of parts of the website.

19. AUTOMATED DECISION-MAKING AND PROFILING

- 19.1. FlareX may use automated tools for identity verification, sanctions screening, fraud detection, transaction monitoring, cybersecurity, risk assessment and operational processes. Where a decision contemplated by section 71 of POPIA is based solely on automated processing and has legal consequences for a data subject or affects the data subject to a substantial degree, FlareX will apply the safeguards and exceptions required by POPIA.
- 19.2. Where applicable, those safeguards may include measures to allow an opportunity for human intervention, representation by the data subject and a mechanism to challenge the outcome, subject to legal, security and regulatory constraints.

20. RETENTION AND SECURE DISPOSAL

- 20.1. FlareX will retain personal information only for as long as necessary for the purpose for which it was collected or subsequently processed, or for as long as required or permitted by applicable law, regulation, contractual obligations, regulatory requirements, audit requirements, dispute resolution or the establishment, exercise or defence of legal claims.
- 20.2. Retention periods may therefore differ depending on the type of information and the applicable legal or regulatory obligation. When information is no longer required, and there is no lawful basis for continued retention, FlareX will securely delete, destroy or de-identify it in a manner that prevents reconstruction in accordance with its records-retention procedures.

21. DATA SUBJECT RIGHTS

- 21.1. Subject to the conditions, exceptions and limitations in POPIA and other applicable law, a data subject may exercise rights including:
- 21.1.1. the right to request confirmation of whether FlareX holds personal information about the data subject and to request access to that information;
 - 21.1.2. the right to request correction or deletion of personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or unlawfully obtained, subject to POPIA;
 - 21.1.3. the right to object to processing on reasonable grounds relating to the data subject's particular situation, where section 11 permits such objection;
 - 21.1.4. the right to object to the processing of personal information for direct marketing by means of unsolicited electronic communications;
 - 21.1.5. the right to withdraw consent where processing is based on consent; and,
 - 21.1.6. the right to lodge a complaint with the Information Regulator where the data subject believes that POPIA rights have been infringed.
- 21.2. Requests should be made to the Information Officer using the contact details in section 24. FlareX may require sufficient information to verify the identity and authority of the requester. Access requests are subject to POPIA and PAIA procedures, applicable exemptions and any lawful fees.

22. REQUESTS, COMPLAINTS AND INTERNAL HANDLING

- 22.1. FlareX will maintain procedures for receiving, recording, verifying, assessing and responding to requests and complaints concerning personal information. Requests will be handled within the timeframes and in accordance with the procedures prescribed by applicable law.
- 22.2. Where FlareX cannot comply with a request, it will provide the data subject with an appropriate explanation to the extent required by law. Nothing in this Policy limits a data subject's statutory rights or the powers of the Information Regulator.

23. PAIA AND ACCESS TO INFORMATION

- 23.1. Requests for access to records, including requests for access to personal information contemplated by POPIA, may be subject to PAIA and FlareX's PAIA Manual. The PAIA Manual contains information about FlareX's records, the procedure for making requests and the applicable statutory requirements. The latest version should be made available to requesters in accordance with applicable law.

24. CHANGES TO THIS POLICY

- 24.1. FlareX may amend this Policy from time to time to reflect changes in legislation, regulatory requirements, technology, business activities, processing operations, security measures or best practice. Material changes will be communicated through appropriate channels, and the latest approved version will be made available on the FlareX website or otherwise on request.
- 24.2. This Policy will be reviewed at least annually and whenever there is a material change to the way FlareX collects, uses, stores, discloses or transfers personal information.

25. INFORMATION OFFICER AND CONTACT DETAILS

- 25.1. The Information Officer is responsible for supporting FlareX's compliance with POPIA and PAIA and for handling privacy-related enquiries and requests.

Information Officer	Matthew Morgan
Physical address	Sasol Building 50 Katharine Street Sandton Johannesburg 2196
Email	Matthew@flarex.com
For the attention of	Matthew Morgan
Privacy requests	Requests, corrections, objections, consent withdrawals and privacy complaints may be submitted to the Information Officer using the above email address.

26. COMPLAINTS TO THE INFORMATION REGULATOR

- 26.1. A data subject who believes that FlareX has infringed their rights under POPIA may lodge a complaint with the Information Regulator in accordance with the applicable complaint procedure. The Regulator's current contact details and electronic services should be obtained from its official website.

26.2. Information Regulator of South Africa

Website: <https://infoeregulator.org.za/>

General enquiries: enquiries@infoeregulator.org.za

Telephone: 010 023 5200

POPIA complaints: POPIAComplaints@infoeregulator.org.za

27. DOCUMENT VERSION CONTROL

Document owner	Information Officer
Version	2.0
Effective date	23 September 2026
Review frequency	At least annually and sooner there is a material legal, regulatory, operational or technology change
Primary legislation	Protection of Personal Information Act 4 of 2013 (POPIA)
Approved by	Chief Compliance Officer