VIKTORION

GDPR / Privacy

Version 2.0
April 2026

Viktorion.com is owned and operated by Victory FX Limited, a private limited company incorporated in the United Kingdom under company number 06634847, with registered address at 78 York Street, London, W1H 1DP.

Contents

1. Introduction

This policy (“Privacy Policy”) outlines how **Viktorion TS** (the "Company") processes Personal Data of natural persons. This Privacy Policy applies to the following category of natural persons:

- you are either a current or potential client of the Company, or
- you have expressed an interest in or inquired about the Company’s products / services, or
- you represent or are the administrator of a client of the Company, or
- you have provided or may potentially provide guarantees, indemnities or other securities to the Company, or
- you are an authorised representative / agent / introducer / statutory director / secretary / contact person or shareholder / beneficial owner of a legal entity which has or intends to create a business relationship with the Company, or
- you have provided or are requested to provide references or confirmations for a client or a member of staff of the Company, or
- you are connected with a client or a member of staff or a business associate of the Company and your Personal Data is provided under a regulatory obligation e.g. to manage possible conflicts of interest and other regulatory obligations, or
- you have been in the past any of the above (please refer to section 7), or
- you now have or had any business relationship with the Company in the past including being an employee, a shareholder or bondholder, or
- you applied for an opening / job position in the Company, or
- you were contacted to discuss potential business with the Company; or
- your Personal Data have or may in the future be lawfully obtained and Processed by the Company in the normal course of its business.

Processing may take place at Group level as provided under the General Data Protection Regulation 2016/679 (GDPR), where a legitimate interest is justified. Group being the Company and any legal entity which is considered a subsidiary pursuant to Companies Law Cap. 113.

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such Processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union or Member State law;
(**"Data Subject"**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"Processor" means a natural or legal person, public authority, agency or other body which processes

Personal Data on behalf of the Controller;

The Personal Data Processed by the Company depends on your categorization and or classification as a client or potential client of the Company as well as on the products or services you request from the Company, or the Company agrees to provide to you, from time to time.

In all cases, the Company is committed to processing your Personal Data in compliance with the provisions of the GDPR. The rights provided to you by the GDPR in relation to the Processing of your Personal Data by the Company are also described in this Privacy Policy.

2. Who is responsible for Processing your Personal Data

Your Personal Data will be held by **Victory FX LTD**, a United Kingdom registered company under registration number 06634847.

The Company can act as both a Personal Data Controller and a Personal Data Processor depending on the circumstances and the nature of its business activities.

Where the Company determines the purposes and means of Processing Personal Data, it is acting as a Controller. For example:

- Marketing and Communication: where the Company processes Personal Data for its own marketing purposes, such as sending promotional emails to clients, it determines the purpose (marketing) and means (which data to use, how to contact clients) and thus acts as a Controller.
- Internal Operations: For activities such as HR management, payroll, or internal financial audits, where the Company processes Personal Data of employees or clients for its operational purposes, it acts as a Controller.
- Compliance with Regulatory Obligations: where the Company processes Personal Data to comply with legal obligations, such as anti-money laundering (AML) checks, tax reporting, or Common Reporting Standards (CRS) obligations, it acts as a Controller. The Company decides how to process the Personal Data to meet regulatory requirements

On the other hand, where the Company processes Personal Data on behalf of another entity (usually a data Controller) and does not determine the purposes and means of Processing, it is acting as a Processor:

- Custodian Services: When the Company provides custodian services for another investment firm or institution and processes the Personal Data related to the assets being held but does so under the instructions of the client or another firm, it acts as a Processor.

Contacting the Company about this policy or any matter regarding your Personal Data

If you wish to contact the Company about the Processing of your Personal Data, you may do so using the following contact details: **Viktorion TS,** info@viktorion.com, compliance@viktorion.help .

3. What Personal Data is Processed and from which sources

The Personal Data Processed may be any or all the following types:

Data type	Description
Identification data including national identification numbers	Information which can directly identify you such as name, surname, date of birth, gender, place of birth, citizenship and identification numbers or codes given or issued by a governmental service such as national social insurance number, tax identification code, ID number, Passport number, Driver's license number and other Personal Data of similar type.
Contact	Contact details such as telephone number, home address, work address and personal email address.
Financial	Information on your personal wealth including your assets, details of the assets, streams of incomes, expected incomes, personal financial position, salary, economic status, account numbers, IBAN and other financial information. In case you receive or applied to receive investment services, financial data to be obtained include knowledge and experience with MiFID II products (i.e., derivatives, shares, bonds, funds and interest rate/currency products), your investment strategy and scope, details of your personal investment portfolio, personal financial objectives.
Socio-demographic	This includes details about your work or profession, nationality, level of education, marital status and where you fit into general social or income groups.
Transactional	Details about payments to and from your accounts with the Company including information of third parties from whom money are received or transferred to.
Contractual	Details about the products or services we provide you with. This includes data concerning your accounts. Specific information relevant to existing/previous accounts.
Locational	Data we get about where your location, in particular when accessing our website, portals and trading platforms and use our products and services. Such data may come from your mobile phone, the address and IP where you connect a computer to the internet, or a shop where you buy something with your card.
Behavioral	Details about how you use our products and services.
Technical/Digital	Details of the devices and technology you use, your digital activity and systems logs which are captured by the Company's information technology systems when you use them, IP addresses and the credentials you use to connect to our digital platforms available or internal systems in the case of employees.
Communications	What we learn about you from letters, emails and conversations/meetings between us.
Social Relationships	Your family, associates and other relationships you declare for the purposes of our business relationship.
Documentary	Details about you that are stored on documents in different formats, or copies of them. This could include things like your specimen signature, passport, identity card, driver’s license or birth certificate.
Video and sound recordings	Video footage recorded by the CCTV system of the Company in which you may be captured when you visit the Company, or voice call recordings when you call us or video recordings when you make an online meeting with us.
Special categories of Personal Data	The law treats some types of Personal Data as special. These include Personal Data concerning data relating to criminal convictions and offences. The Company may, also, process data relating to criminal convictions and offences as part of the Company's initial and periodic review, as required by law. The legal basis used for such Processing is the Legal Obligation (refer to section 5 below). Through all financial transactions, various types of behavior patterns can be revealed, which may include special categories of Personal Data. Therefore, there is a good chance that the Company when Processing information about financial data transactions will also process special categories of Personal Data (e.g., When you pay for medical costs to a doctor of certain specialization).

The Company collects Personal Data from the following sources:

- Directly from you:

- When you apply for the Company's products and services
- When you contact the Company in writing or over the telephone, via email, online, or enter the premises of the Company
- When you use the Company's websites and platforms online through devices, including mobile device applications and Application Programming Interface (APIs)
- When you access the Company's premises
- In financial reviews and interviews
- In surveys
- By participating in Company competitions or promotions
- When interacting with the Company through any social media platform
- When submitting a review online or through any other medium
- When necessary, in the context of the business relationship between you and the Company

- Indirectly, for example through:

  - Your authorised representatives
  - Persons/Organisations introducing you to the Company
  - Persons providing references for you, including your previous employers
  - Clients or members of staff providing your contact details in order for the Company to receive references from you or as part of the reporting of a conflict of interest
  - The legal entity you represent or in which you act as agent/ introducer / statutory director / secretary / contact person / shareholder / beneficial owner or any other role which is necessary for the execution of the Company's business operations with that legal entity

- From other publicly accessible sources such as:

  - the Land Registry Offices
  - the Registrar of Companies
  - the Bankruptcy Register
  - the UBO Register
  - other Commercial Registers
  - the Press or the Media
  - the Internet and Social Media
  - any equivalent body or authority in your country of residence

- Other resources such as:
  - other financial institutions, card associations, payment solution providers (PSPs), electronic money institutions (EMIs)
  - Other service providers such as Refinitiv, iSpiral, and GB Group Plc, for the purposes of receiving information necessary for our enhanced due diligence obligations under the AML Law
  - Criminal records
  - CCTV systems for security, fraud, and crime prevention

4. Why do we Process your Personal Data and on what legal basis

(a) Legal Basis

The law allows the Company to process Personal Data, including sharing Personal Data outside the Company, only if the Company has a valid reason to do so. Specifically, the Company must have one or more of the following reasons to use your Personal Data:

To fulfil a contract you have with the Company or to take any steps, at your request, prior to entering into a contract with the Company - The Company processes your Personal Data in order to provide you with investment services, in accordance to the contracts concluded with you and/or in the course of your application prior to the conclusion of a contract in order to complete your trading account opening and/or to execute your orders following the creation of your trading account.

When it is the Company's legal obligation – The Company processes your Personal Data in order to comply with requirements of the legal and regulatory framework governing its operations including but not limited to investment services legislation, anti-money laundering legislation, tax legislation and regulations, directives/ guidelines issued by the Company's regulators (including the Mauritius Financial Services Commission, the European Securities and Markets Authority, the Central Bank of Mauritius, the European Banking Authority, Tax Authorities, domestic regulatory authorities in other Member States, and any other authority of competence).

When it is in the legitimate interests of the Company or another person with whom the data are shared – The Company may process your Personal Data in case it has a legitimate interest to do so, provided this interest does not unfairly go against what is right and best for you. A legitimate interest is when the Company has a business and/or commercial reason to use your Personal Data. When the Company bases the Processing of your Personal Data on legitimate interest you have the right to object at any time to such
Processing, on grounds relating to your particular situation. The Company shall no longer process your Personal Data unless it demonstrates compelling legitimate grounds for the Processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims. Where Personal Data are Processed for the purposes of direct marketing, you have the right to object to such Processing, including profiling to the extent that it is related to such direct marketing, whether regarding initial or further Processing, at any time and free of charge. Where you object to Processing for direct marketing purposes, the Personal Data shall no longer be Processed for such purposes.

When you consent to the use – The Company may base the Processing on your consent if such consent is free, specific, and has been given after you have been clearly informed about the details of the Processing. You have the right to withdraw your consent at any time, but such withdrawal does not affect the legality of the Personal Data Processed prior to the withdrawal.

When it is in the public interest or in the exercise of official authority vested in the Company – The Company may process your Personal Data when it is necessary for the public interest by virtue of official authority granted to the Company and provided that the Processing is performed lawfully and fairly, in a clear, precise and transparent manner.

(b) Purposes of Processing

As detailed above, Processing is only lawful if it meets one of the following legal bases:

- **Consent**: The data subject has given explicit consent for one or more specific purposes.
- **Performance of a Contract**: Processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering into a contract.
- **Legal Obligation**: Processing is necessary to comply with a legal obligation to which the controller is subject.

- **Public Interest or Official Authority**: Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- **Legitimate Interests**: Processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Indicatively, the Company processes your Personal Data for the purposes under the legal basis marked respectively below.

i. Provision of services

We need to process your Personal Data for the Company:

(a) to be able to review your trading account opening application for the Company's products and services;
(b) if approved, to provide to you any of the investment services the Company is authorized to provide, from time to time;
(c) execute/accept payments or other payment services;
(d) to attend to requests directed to customer support through emails, phone calls, or online;

Personal Data Processed shall be restricted to the necessary data for the purposes of the service(s) received or provided.

Your Personal Data may be Processed for any service requested by you including the exercise of your rights under GDPR as detailed in section 8 below as well as the Processing of your applications submitted via the Company's webpage.
Legitimate interest pursued:

- *To perform company searches by third-party service provider*
- *To process the Personal Data of third parties participating in payments to/from clients*
- *To manage payments through third-party service providers*
- *To obtain technical support on Company systems from third-party service providers (the Company may process Personal Data when troubleshooting/updating systems)*
- *To facilitate the conclusion of a service using third parties such as PSPs or EMIs*
- *To record calls with nonclients when they make inquiries from the Company's Call Center or online support on the Company's website.*
- *To give access to clients' representatives on various Company's channels/applications to serve the purposes of the Company's clients*

To provide general information about the Company and its products.

ii. Comply with Anti-Money Laundering (AML) regulatory framework

Your Personal Data will be Processed to comply with the Company's regulatory obligations under AML.

Your Personal Data / economic profile and transactional activity will be reviewed and updated periodically. The Company has to perform due diligence and investigate the source, origin, and destination of the funds of the transactions you carry out through the Company,

Any activity or transactional behaviour that is inconsistent with your profile will be further investigated by the Company.

The Company uses providers such as Refinitiv, iSpiral, and GB Group Plc to obtain information concerning existing and potential clients to perform enhanced due diligence where required under applicable AML Laws. Legitimate interest

pursued:

- *To exercise due diligence in relation to new clients' onboarding or to existing clients at the review of the client relationship or their transactions by carrying out searches in available databases either directly or through third party service providers.*

To defend the Company in litigation procedures.

iii. Comply with Regulatory Reporting requirements and other legal obligations

Your Personal Data is Processed by the Company for compliance with its regulatory obligations.

The Company is obliged to report to regulators several reports, some of which may contain Personal Data.

The Company also reports to tax authorities in line with the legal framework of the Republic of Mauritius, the EU, and other countries such as USA for FATCA[1], where applicable.

The Company is obliged to comply with court orders.

The Company will assist law enforcement authorities in carrying out investigations or gathering evidence. Legitimate interest pursued:

- *To protect the Company from fraud or crime*

iv. Manage risks

The Company, as part of its day-to-day operations, manages risks and ensures that our clients, counterparties, stakeholders, and the Company and its employees are properly safeguarded against those risks. For the purposes of managing those risks, it might become necessary to Process your Personal Data (e.g. observation of CCTV systems for the purposes of security, fraud, and crime prevention, maintaining log books of visitors to the Company's buildings when validating financial models used by the Company, when monitoring credit risks, when overviewing the overall quality of the investment portfolio, when investigating threats / vandalism / robbery / terrorist acts or aggressive behaviour against members of staff, when enhancing IT security, when handling conflict of interest. Indicatively the risks managed include:

- Physical access to our buildings
- Crime and fraud
- Cyber & Information security
- Operational risks
- Breaches and other incidents
- Regulatory risks
- Client risks
- Reputational risks
- Legal risks
- Conflict of interest

Legitimate interest pursued:

[1] The Foreign Account Tax Compliance Act (FATCA), which was passed as part of the HIRE Act, generally requires that foreign financial Institutions and certain other non-financial foreign entities report on the foreign assets held by their U.S. account holders or be subject to withholding on withholdable payments.

- To implement proper monitoring tools to prevent malicious activity.
- To investigate information security incidents and/or specialised systems used by the Company.
- To monitor the access to the Company's premises and other locations to ensure security of staff, clients, visitors and the Company's assets.
- To keep track of visitors who enter the Company's premises for security purposes.
- To assess incidents or threats of crime in the Company's premises or on the Company's assets or people.
- To manage possible conflicts of interest.

v. Preparation of Financial Statements/Management of costs and income

We may process your Personal Data during the preparation of our financial statements, during assessment, management and reporting of costs and income, during setting up the models for the parameters of provisions (including at group level).

Legitimate interest pursued:

- *To facilitate the financial affairs of the Company*

vi. Internal Operations

Your Personal Data will be processed by the Company while carrying out administrative tasks and its internal operations. Examples of the Processing taking place include:

- monitoring data quality and accuracy.
- providing operational support to the client-front units.
- management of client relationships through the CRM-Client Relationship Management system.
- through call & video recordings of communications with you.
  issuing access cards or devices to monitor who enters or exits the Company's premises and common areas such as the lift.
- preparing & using internal reports and lists (such as the Insider List required under the Market Abuse Regulation), which may include your Personal Data which are used by the relevant units of the Company for the purposes of executing their work.
- during the handling of requests which require expert opinion such as legal opinion, or opinion from other control functions and experts such as Compliance Unit, Data Protection Office, Information Security, Tax, IT, and Health and Safety (Organisation).
- checking the smooth operation of processes i.e., content of letters, announcements or communications.
- for anonymization and for statistical analysis of the usage of the Company's products and services and/or for testing the Company's products and services as part of the Company's Product Governance Policy and for the purposes of further product / service enhancement or development of new products / services aiming value added to clients.
- maintaining and publishing internally, with access as deemed necessary, the names and other necessary details of approved counterparties i.e., auditors, lawyers, translators or other counterparties such as technical support counterparties, cleaners, food services, groceries distributors, landlords for rented property, etc.
- for collecting and recovering money that is owed to the Company.
- defending the Company' legal rights.
- for responding to third parties, provided that these third parties are authorised to receive such information.
- to respond to regulatory inquiries.
- for process automations.

Additionally, the Company may share your Personal Data with third parties as listed in sections 5 and 6 of this Privacy Policy for the internal operation purposes listed below:

- to enable the Company to defend itself in court actions – to external legal advisors.
- to enable the Company to comply with court or regulatory orders – to regulators or the police or other law enforcement authorities.
- to enable the Company to manage vendor relationships in outsourcing arrangements - to third-party vendors including cloud service providers and Information Technology support.
- to insure the Company, its employees, directors and officers, and its assets.
- for the Company to fulfill its regulatory and reporting obligations and update FSC's Portal.

Furthermore, the Company may obtain information from third-party sources as listed in section 3 of this Privacy Policy for the internal operation purposes listed below:

- to establish the ownership and status of assets if a client declares passive income as their source of income – from the Land Registry / Registrar of Companies or equivalent bodies
- to establish the ownership structure and status of corporate clients of the Company - from the Registrar of Companies
- to screen for sanctions and other negative information on clients – world check and/or other relevant databases.

Please refer to the purpose "*Comply with Anti-Money Laundering (AML) regulatory framework" for more details.*

Legitimate interest pursued:

- To ensure that data kept is accurate and up to date and to check for any discrepancies.
- To record calls for better service / improvement of services.
- To provide support / advice to departments of the Company, where requested.
- To be able to communicate, when necessary, with the third-party providers.
- To monitor the Company's deposit and loan portfolio for the purposes of liquidity, capital adequacy and strategy monitoring.
- To ensure that automated processes run smoothly e.g., the interest is correctly charged.
- To be able to provide reports and information to the Board and its Committees in order to successfully fulfil their obligations.
- To check/confirm data to be sent to clients.
- To produce reports for business monitoring and growth.
- To be able to investigate client claims, complaints aor gather information for court cases.
- To develop new products and services or enhance existing.
- To ensure that divisions' strategic targets are met by using external support and expertise.
- To improve processes in terms of cost, time and quality.

When sharing your Personal Data with third parties or when receiving your Personal Data from third parties, the Legitimate Interests pursued are listed under the column "Purposes of Processing".

vii. Administration of Company systems

Your Personal Data may be processed to ensure the smooth operation of the systems utilised by the Company in its operations i.e. to administer user access rights, for troubleshooting, configuration, infrastructure management, data integration between systems used, administer parameters and proxies on web traffic and email gateway. Legitimate interest pursued:

- To be able to administer the Company's systems to ensure smooth and accurate operation.
- To provide access to Company systems where necessary for members of staff to be able to perform their tasks and duties.
- To access data in systems to identify system glitches.
- To provide access to third-party service providers to support the IT Department with workload and for the development and implementation of new features in various systems.

viii. Audits / Investigations

The Company may process your Personal Data during audits/investigations carried out either by internal auditors and other control functions or by external auditors and/or regulators on the Company's operations, including the Commissioner for Personal Data Protection.

Legitimate interest pursued:

- To be able to enhance the Company's controls and to outsource the internal audit of Information Technology functions and or other departments, where external expertise is required.

ix. Responding to complaints

The Company may process your Personal Data when a complaint is submitted (including complaints in relation to harassment) for the purposes of responding and/or handling that complaint. Legitimate interest pursued:

- To process any Personal Data provided by you and/or held by and/or given to the Company in order to respond to and/or handle the complaint received.

x. Communication

The Company may process your Personal Data for the purposes of communicating with you. Some examples are the following:

- to provide general information about the Company, such as working hours.
- to provide specific information for a product or service you hold or are receiving
- to provide you with statements, charges analysis, transactional activity, trading history etc.
- for marketing purposes such marketing via email, chats, and live calls. to inform you of the results of campaigns / competitions / draws to which you participated.
- to inform you of cases of fraud and or breaches.

The Company may also communicate with natural persons who are not clients of the Company:

- whose Personal Data were obtained in conferences e.g. to promote Company's products and services
- If your contact details have been obtained by a member of staff for the purposes of contacting you on emergency situations or by a member of staff/prospect member of staff or client for the purpose of receiving references.
- for direct marketing (even if the Personal Data/contact details are available to the public).
- to inform you of the results of campaigns / competitions / draws to which you participated.
- to inform you of cases of fraud and or breaches.

The Company may also communicate with natural persons who are not clients of the Company:

- whose Personal Data were obtained in conferences e.g. to promote Company's products and services
- If your contact details have been obtained by a member of staff for the purposes of contacting you on emergency situations or by a member of staff/prospect member of staff or client for the purpose of receiving references.
- for direct marketing (even if the Personal Data/contact details are available to sources open to the public)

If you are an investor or market analyst or participant to provide updates/resolving queries in relation to the financial performance of the Company, in accordance with your requests or if you are a shareholder or bond holder receiving notifications in accordance with legal requirements or generally.

Legitimate interest pursued:

- To communicate with clients in relation to general information on Company issues, or specific information for a product/service of the client, or for general campaigns to inform clients about similar products/services of the Company.

xi. Competitions/ Promotions

The Company may carry out promotional and rewarding competitions on social media. Your Personal Data may be Processed by the Company for the purposes of the competitions in accordance with the terms disclosed from time to

time in relation to the specific competition, provided that you decide to participate.

- The Company may also process your Personal Data during competitions / campaigns if you are an existing client of the Company using its products/ services to reward you for your commitment and preference to the Company's products. The campaigns may be executed via any of your contact.

Legitimate interest pursued:

- To promote the usage of the Company's products and reward clients through the opportunity to win gifts and benefits.

xii. Record keeping

The Company needs to keep record of its activities as required by the regulatory framework and/or to defend its legal rights and interests pursued.

- The basis for Personal Data retention and record keeping arises predominantly from the legal obligations of the Company and partly from its legitimate interest. You may refer to the specific paragraph in this Privacy Policy with regards to the data retention periods.

Legitimate interest pursued:

- Outsourcing for cost-saving and expert services.

xiii. Cookies

When you visit our website / platform or use our products online (via MT5, MT4, or cTrader) our system Processes information about your visit such as your IP address and your browser type. You can manage these cookies in accordance with the Cookies Policy available to you on the Company's website Legitimate interest pursued:

- to monitor and analyse the functionality and accessibility of the Company's webpage and applications and enduser preferences.

(c) Profiling and Automated decision making

"**Profiling**" means any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse aspects concerning that natural person's, economic situation, personal preferences, interests, behaviour, location or movements. An example of Profiling is the client risk assessment and categorization.

Profiling may involve three distinct stages: a) Personal Data collection; b) automated analysis to identify correlations; c) applying the correlation to an individual to identify characteristics of present or future behaviour.

The Company does not make decisions solely on the basis of automated Processing; however, part of your Personal Data may be automatically Processed as part of our assessment of certain personal aspects (profiling), indicatively for the following purposes:

a) Economic profile and ability to afford the risk of losing the funds traded.
b) Assessments for the purpose of combating money laundering and fraud.
c) Marketing of new products and services of the Company, if consent was lawfully obtained.

5. Who receives your Personal Data

5.1. Within the Company

Within the Company, access to your Personal Data is given exclusively on a need-to-know basis to those officers who require such access to perform the Company's contractual, legal obligations and other internal activities.

5.2. Outside the Company

Access to your Personal Data may also be given to **third-party service providers and agents employed by the Company** to enable more efficient and effective execution of its business operations, provided that an appropriate legal basis exists. Except where they act as separate Controllers, service providers and agents appointed by the Company are required to follow the Company's instructions in relation to the Processing of Personal Data, provide written assurances that it processes the Personal Data in accordance with GDPR and the information shared will be restricted to the minimum necessary for the specified and explicit purposes.

These are mainly organisations from the categories listed below:

- Credit Institutions, Financial Services Institutions, Payment Solution Providers and Electronic Money Institutions
- Visa / Mastercard / JCC / SEPA Direct Debit Scheme, other payment service agents and participating merchants
- Third Party Providers (TPP) where APIs are used at the request of the client
- Fund Managers / Trustees / Agents for reporting (such as those required under MiFID II)
- Affiliates
- Couriers
- IT systems/solutions providers and cloud service providers
- Insurance Companies / Re-insurance agents
- Advisory and professional service providers
- Auditing service providers / Forensic Auditors / Statutory Auditors
- Legal Advisors
- Companies offering marketing services /advertising agencies/ conference organizers
- Record-Keeping companies
- Printing companies
- Providers of data screening services for anti-money laundering purposes
- CCTV system providers
- Other service providers supporting any of the operations of the Company.

The Company may be required to share your personal information **with regulatory and other authorities and public bodies** in Mauritius and the European Union, either under a legal obligation or based on the Company's legitimate interests:

- The Financial Services Commission
- The police and MOKAS and other international or domestic law enforcement authorities.
- Tax authorities
- Financial Ombudsman
- Commissioner for Personal Data Protection
- Other regulators, authorities and public bodies insofar as a statutory or official obligation exists.

The Company may, also, share your personal information with potential or actual **investors / buyers of shares in the**

Company. Specifically, the Company may choose to sell, transfer, or merge parts of its business, or assets, or the Company may seek to acquire other businesses or merge with them. During any such process, the Company may share your Personal Data with interested parties. The Company will only do this if the other parties agree to keep your Personal Data safe and private. In any such case you will separately be notified in accordance with the requirements of the relevant regulatory framework. Upon completion of the relevant transaction, the buyer / investor will become an independent Controller of your Personal Data transferred to them by the Company.

Additionally, the Company may have a legitimate interest in transmitting your Personal Data **within the Group** for internal administrative purposes and / or a legal obligation to do so i.e. for group regulatory reporting.

6. Transfer of Personal Data to third countries or international organisations

The Company will only transfer your Personal Data to a country outside the EEA (a "third country"):

- If this is required for the execution of your orders (for example, executing ana client order through a broker outside EU);
- if this is prescribed by law (for example, reporting obligations under tax law);
- in the context of data Processing undertaken by third parties on behalf of the Company and according to the Company's instructions.

If the Company does transfer your Personal Data to a third country, the Company will make sure that your Personal Data is protected in the same way as if it was being used in the EEA. The Company will ensure at least one of the following bases apply:

- Transfer it to a third country with privacy laws that afford the same protection as the EEA, as certified by an adequacy decision of the European Commission.
- Transfer it to organisations that comply with binding corporate rules, or an approved code of conduct or certification mechanism that requires its protection to the same standards as applicable in the EEA.
- Put in place a contract with the recipient which includes the standard data protection clauses adopted by the European Commission or adopted by the supervisory authority and approved by the European Commission.
- Where the recipient in the third country has signed up to a code of conduct, which has been approved by a competent supervisory authority. The code of conduct must include appropriate safeguards to protect the rights of individuals whose Personal Data transferred, and which can be directly enforced.
- Where the recipient in the third country has a certification, under a scheme approved by a competent supervisory authority. The certification scheme must include appropriate safeguards to protect the rights of individuals whose Personal Data transferred, and which can be directly enforced.

In the case where none of those bases apply, your Personal Data may still be transferred to a third country under the following conditions/ derogations, where:

- you explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between you and the Company, or the implementation of pre-contractual measures taken at your request;
- the transfer is necessary for the conclusion or performance of a contract concluded in your interest between the Company and another natural or legal person;
- the transfer is necessary for the establishment, exercise or defense of legal claims;
- the transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent.

Where a transfer could not be based on any of the above, a transfer to a third country or an international organisation may take place only if:

- the transfer is not repetitive,
- concerns only a limited number of Data Subjects,
- is necessary for the purposes of compelling legitimate interests pursued by the Company which are not overridden by the interests or rights and freedoms of the Data Subject, and
- the Company has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of Personal Data.

In such a case the Company shall inform the supervisory authority of the transfer and the relevant persons whose Personal Data will be transferred on the fact of the transfer and the compelling legitimate interests pursued.

Where transfers are made, as above, the Company conducts Data Transfer Impact Assessments and regularly monitors the process to ensure continued protection.

6.1 Cloud Services

The Company uses cloud technology to store your Personal Data referred to under section 4 above. The cloud service providers used by the Company and their data centers, are located in the European Union and thus bound by the GDPR requirements.

Despite this, there are cases where Personal Data may be transferred to or accessed from a third country for the purpose of the provision of the services outsourced or, if required by law. In such a case the Company shall ensure that the relevant safeguards as mentioned in section 6 above will apply.

The Company ensures contractually that the cloud service provider will apply principles of data minimization and will not use or otherwise process your Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or (d) any other purpose, unless such use or Processing is in accordance with Company's documented instructions.

In case where special categories of Personal Data (Personal Data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation) will be transferred on cloud, the Company will notify the Commissioner for Personal Data Protection prior to such transfer if required by the applicable regulatory framework i.e. when the cloud service provider transfers the special categories of Personal Data to a third country.

Retention of Personal Data on cloud shall be in line with the general retention policy of the Company as described in section 7 below.

You may still exercise your rights as disclosed in section 9 below in relation to this Processing activity.

7. For how long your Personal Data is retained by the Company

7.1. Existing relationships

The Company processes and stores your Personal Data as long as you are a client of the Company and/or you maintain any type of relationship with the Company and such Processing is necessary for the performance of the Company's contractual obligations, including the period prior to the conclusion of the contract with you (i.e., pre-contractual

arrangements) and other legal obligations.

7.2. Terminated relationships

After you stop being a client of the Company or you stop maintaining any type of relationship with the Company, the Company will keep your Personal Data for a period of **7 (seven) years** from the date of termination for the following reasons:

- To maintain records according to rules that apply to the Company such as under applicable tax, investment services and money laundering laws and regulations.
- To respond to any questions or complaints.
- To demonstrate if needed that the Company treated you fairly.
- To preserve evidence that may be needed for the establishment, exercise or defence of legal claims.

It is clarified that if the Company holds your Personal Data because you are related to a client of the Company (e.g., you are a representative, beneficial owner, officer or guarantor), the Company will keep your Personal Data for any of the above reasons for **7 (seven) years** after the end of the relationship of the Company with the relevant client.

We may keep your Personal Data for longer than the said period:

- If we cannot delete it for legal and/or regulatory and/or technical reasons. If we do so, we will ensure that your privacy is protected, and the Personal Data is used only for the purposes stated in paragraph 4 above. For example, by the expiration of the above period, there are on-going judicial proceedings with the Company concerning you directly or indirectly. In such a case the above period for the retention of the Personal Data will be extended until a final judicial decision is issued or the a judgement is fully performed, whichever comes earlier.
- For research or statistical purposes. If we do so, the Company will make sure that any data will be pseudonymized or anonymized and in aggregate form, as the case may be, to ensure your privacy is protected, and the data is used exclusively for research or statistical purposes.

7.3. Prospective Clients

In case you provide us with Personal Data for the purposes of becoming a client of Company but for any reason whatsoever you decided to withdraw your account opening application prior to an approval or rejection from the Company, your personal data will be kept for a period of **6 (six) months** from the date of notification of your withdrawal of your application, in accordance with directives/guidelines issued by the Mauritius Commissioner for the Protection of Personal Data. If you withdraw your application but file a complaint for whatever reason, your personal data will be retained until any such complaint is permanently resolved.

Where your account opening application has been rejected by the Company for whatever reason, your Personal Data will be retained for a period of **12 (twelve) months** from the date of notification of your rejection to fulfill the Company's reporting obligations as well as demonstrate fair treatment and adherence to the Company's internal policies and procedures such us its product governance and target market.

7.4. Other provisions

Personal Data gathered during a recruitment process will be deleted following completion of the screening for the specific opening, unless the job applicant provided their consents to their personal data to be kept on file for future openings. In any event, the Company will retain the Personal Data for a period of **12 (twelve) months** from the date of the job applicant's notification of unsuccessful application.

In all respects, where a shorter or longer time period for the retention of Personal Data is provided for by law or regulatory acts, the retention period mentioned above will be reduced or increased accordingly.

7.5. Consequences for refusal to provide your Personal Data

Failure to provide Personal Data which is legitimately required by the Company will result in the Company not being able or allowed to commence or continue any business relationship with potential or existing clients.

7.6. Table of Data Categories and corresponding retention periods

Data Category	Type of Individual	Data Examples	Retention Period	Legal Basis
Client Data	Clients	Personal details, financial information, investment history, transaction records, all communications.	7 years	Required to comply with Anti-Money Laundering (AML) regulations, tax, and financial reporting obligations. 5–10 years typically required.
Prospective Client Data	Prospective clients	Contact details, investment preferences, correspondence, personal details, financial information	6 months	Retained based on legitimate interest for potential future business. (This refers to the Clients that have created a real / live trading account)
Applicant Data	Job applicants	CV, personal details, interview notes, qualifications	12 months after hiring/rejection decision	Necessary for legal defense against discrimination claims. Periods can be longer depending on local employment laws.
Service Provider Data	Service providers/contractors	Contracts, payment details, contact and personal information	7 years after contract termination	Retained for contractual purposes, audits, and regulatory compliance.
Employee Data (current)	Employees	Personal details, payroll, performance reviews, contracts	Duration of employment + 7 years	Required for employment law, tax, and pension purposes.
Employee Data (former)	Former employees	Employment contracts, termination letters, exit interviews	7 years after employment	Required to defend against legal claims (e.g., wrongful dismissal) and comply with tax and pensions regulations.
KYC & AML Data	Clients, employees, contractors	Identification documents, financial records, communications	7 years	Required to comply with Anti-Money Laundering (AML) regulations, which typically mandate retention for at least 5 years.

Marketing Data	Clients, prospective clients	Email addresses, marketing preferences	Until consent is withdrawn, or after 2 years of inactivity	Retained based on consent; data should be deleted once consent is revoked or after a reasonable period of inactivity.
Health and Safety Data	Employees	Incident reports, health assessments	Duration of employment + 7 years	Required for employment law, legal defense, and insurance claims handling.
Pension and Benefits Data	Employees and former employees	Pension contributions, beneficiary details	Duration of employment + 7 years	Retained for pension and retirement plan compliance, as well as future benefits claims.
Disciplinary and Grievance Records	Employees and former employees	Complaints, warnings, investigation reports	Duration of employment + 7 years	Retained for legal defense purposes and compliance with employment regulations.

8. Data Subjects Rights

The Data Subjects rights under the GDPR are outlined below. Data Subjects may exercise their rights at any time in any of the following ways:

- Contacting support or writing an email to compliance@viktorion.help ;

8.1. Right to access Personal Data

Data Subjects have the right to obtain from the Company confirmation as to whether their Personal Data is being Processed and/or obtain access to their Personal Data held by the Company. Manifestly unfounded, excessive, or repetitive Subject Access Request will be subject to a reasonable fee, in line with Articles 12 and 15 of the GDPR.

8.2. Right to rectification of Personal Data

Data Subjects have the right to question any Personal Data the Company holds about them that they think is wrong or incomplete. If they do, the Company will take reasonable steps to check its accuracy and correct it.

8.3. Right to erasure (“right to be forgotten”)

Data Subjects have the right to have the Company delete or remove their Personal Data in the following circumstances:

- The Processing of the Personal Data by the Company is no longer necessary for any of the reasons the Personal Data was collected and used.
- They have withdrawn their consent and there is no other reason for Personal Data Processing.
- They have successfully objected to the Processing of Personal Data by the Company.
- The Personal Data has been unlawfully Processed.
- Deletion is required by law.

It is clarified that the Company reserves its right to deny the said erasure, if the Processing is necessary for the Company to comply with its legal obligation, for reasons of public interest and/or for the exercise of its legal claims.

8.4. Right to restriction of Processing of Data Subjects Personal Data

Data Subjects also have the right to restrict the Company's use of their Personal Data in the following circumstances:

- pending verification by the Company of Personal Data the accuracy of which they have contested.
- the Processing is unlawful, but they do not want their Personal Data to be erased.
- the Company no longer needed the Personal Data, but they do not want it to be erased because they need it for the establishment, exercise or defense of legal claims.
- pending the Company's assessment where they have objected to Processing intended to safeguard the Company's legitimate interests.

8.5. Right to data portability

Data Subjects have the right to receive their Personal Data from the Company in a structured, commonly used and machine-readable form. You can also ask the Company to transfer your Personal Data in this format to other organisations, where this is technically feasible. This right relates to the Personal Data which you have provided to the Company and which the Company processes electronically in reliance on your consent or for fulfilling the contract between you and the Company. Manifestly unfounded, excessive, or repetitive Subject Access Request will be subject to a reasonable fee, in line with Articles 12 and 15 of the GDPR.

8.6. Right to object

Data Subjects have the right to object to the Company's use of their Personal Data and ask the Company to stop using their Personal Data in any of the following circumstances:

- They have the right to object, on grounds relating to their particular situation, at any time to Processing of their Personal Data which is intended by the Company to safeguard its legitimate interests or to serve the public interest. If they file an objection, the Company will no longer process their Personal Data unless the Company can demonstrate legitimate grounds for the Processing overriding their interests, rights and freedoms or unless the Processing is for the establishment, exercise or defence of legal claims.
- They have the right to object to the Processing of their Personal Data for direct marketing purposes, including profiling. If they lodge such an objection, their Personal Data will no longer be Processed for such purposes.
- They have the right to object to the Processing of their Personal Data for scientific or historical research purposes or statistical purposes, on grounds relating to their situation, unless the Processing is necessary for the performance of a task carried out for reasons of public interest.

8.7. Right to withdraw your consent

Where the Company relies on a Data Subject’s consent for the Processing of their Personal Data, they can withdraw their consent at any time. If consent is withdrawn, the Company will not be able to provide certain products or services to Data Subjects. In any such case, the Company will inform the Data Subject beforehand of the consequences of giving effect to their withdrawal notification.

Please note that the withdrawal of the consent does not affect the legality of the Personal Data Processed prior to the withdrawal nor does it the prevent or prohibit the Company for Processing any Personal Data the Company is under a legal obligation to retain, in accordance with section 7 above.

8.8. Data Subject Access Request (DSAR) Procedure

Where a Data Subject requests access to their rights, the Company will strive to respond as quickly as possible and within a month from the receipt of the request. If the request is complex or there are multiple requests, the response time can increase to up to 3 months.

DSARs can be brought to the Company's attention:

- Writing an email to compliance@viktorion.help

Certain data subject rights might be overridden by legal and regulatory obligations applicable to the Company, thus preventing it from fulfilling the same. Such limitations generally arise when the Company receives a request to delete the Personal Data of a Data Subject, but Anti-Money Laundering and Tax laws applicable to the Company create a legal obligation to retain records for a minimum of 5 years.

9. Data Breach Notification

Timely detection, assessment, and notification of data breaches to minimize risks to individuals and protect their Personal Data is pivotal. The Company's Data Breach Response Plan is outlined below.

9.1. Immediate Identification and Containment

Upon detection or notification of a potential data breach, the Data Protection Officer (DPO) or designated staff member must be informed immediately. The priority is to contain the breach and prevent further loss or exposure of personal data. Steps include isolating affected systems, securing physical access to affected areas, and disabling compromised accounts or services.

9.2. Assessment of the Breach

The DPO or designated team must assess the nature and extent of the breach. This assessment will involve determining:

- The types of data involved (e.g., personal, sensitive, financial).
- The number of affected individuals.
- The potential impact on individuals' rights and freedoms.
- Whether the data was encrypted or otherwise protected.

This evaluation will be completed as quickly as possible to determine whether the breach poses a significant risk to affected individuals.

9.3. Notification to the Mauritius Data Protection Commissioner

If it is determined that the breach is likely to result in a risk to the rights and freedoms of individuals, the company will notify the Mauritius Data Protection Commissioner within 72 hours of becoming aware of the breach. The notification will include:

- A description of the breach and the likely consequences.
- The categories and approximate number of affected individuals and data records.
- The measures taken or proposed to address the breach.
- Contact details of the DPO or point of contact for further information.

If notification to the Commissioner is delayed, an explanation for the delay will also be provided.

9.4. Notification to Affected Individuals

If the breach is likely to result in a high risk to the affected individuals, they will be notified without undue delay. This notification will:

- Clearly explain the nature of the breach.
- Advise individuals on steps they can take to protect themselves, such as changing passwords or monitoring their accounts.
- Describe the actions the Company is taking to mitigate the breach and prevent future incidents.
- Provide contact information for further assistance.

If notifying all individuals requires disproportionate effort, a public announcement may be issued to ensure effective communication.

9.5. Remediation and Review

After the breach has been contained, the Company will conduct a full investigation to understand the root cause and implement corrective measures to prevent recurrence. The incident response team will review existing security measures, policies, and procedures, updating them as necessary to enhance data protection controls.

9.6. Documentation

All breaches, regardless of severity, will be fully documented. The breach log will include details of the incident, the investigation, steps taken, and any communications with the Data Protection Commissioner or affected individuals.

10. Filing a complaint

If you are unhappy with how the Company processes your Personal Data, please inform the Company in any of the following ways:

- Writing an email to compliance@viktorion.help

11. Amendments to the Company's Privacy Policy

This Privacy Policy sets out the information that the Company must provide to you for the purposes of the GDPR. Any information in relation to the Processing of Personal Data contained in this Privacy Policy supersedes any other policies or procedures in so far as any discrepancies might arise.

The Company may revise or update this Privacy Policy from time to time. The new version of this Privacy Policy will be available on the Company's website and shall immediately become valid.

The Company will review this Policy annually or when amendments to applicable laws have taken place.

In case of significant changes the Company will do its best efforts to bring these changes to your attention beforehand. In this context, significant changes might include an increase in retention periods, new rights, or limitations to existing ones. Ultimately, it is your responsibility to check the Company's website for updates.