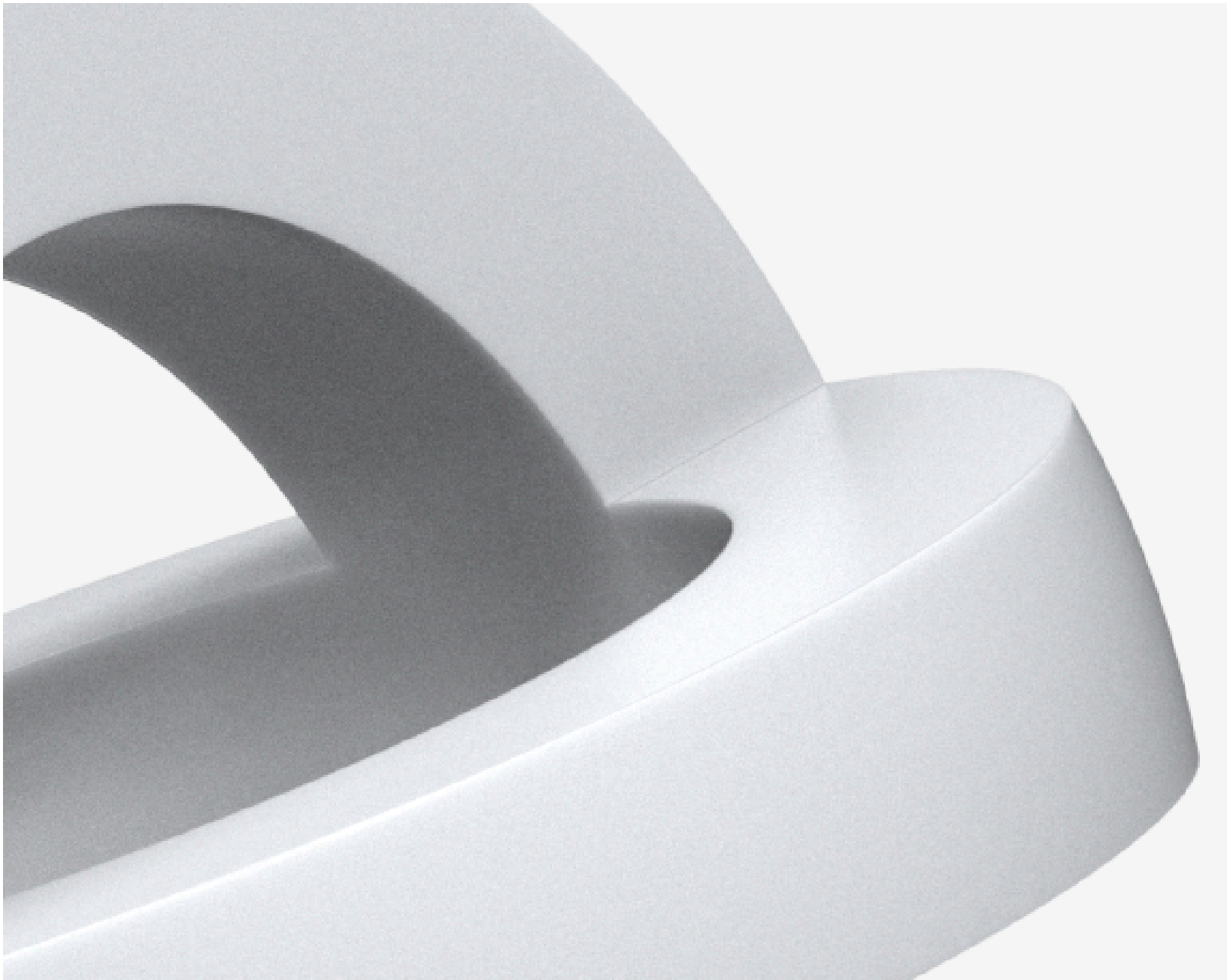
exness

Confidentiality Policy



Definitions

“Company” means Exness (SC) Ltd.

“FCPA 2022” means the Financial Consumer Protection Act 2022 as amended from time to time.

“FSA” means the Financial Services Authority in Seychelles.

“Non-public consumer data” means the data provided by the financial consumer to the Company, which shall not be made available to the public at large.

1. About Exness (SC) Ltd

Exness SC Ltd is a Company incorporated and registered under the laws of Seychelles with registered number 8423606-1. The Company is licensed and regulated as a securities dealer by the Financial Services Authority under license number SD025.

2. Applicable Regulatory Framework and Purpose of this Policy

The formulation and adoption of this Policy is required under section 29(2) of the *Financial Consumer Protection Act of 2022*, according to which the Company shall formulate and adopt adequate confidentiality policies and procedures. The FCPA 2022 came into force with the aim of strengthening consumer protection and confidence when accessing financial services and products in Seychelles.

The policy’s purpose is to formulate the required procedures which ensure protection of non-public consumer information. The policy provides the manner in which the Company, its employees, agents or other relevant parties acting on its behalf, holds, treats and uses information received from actual or potential clients who intend to or partake in the products or services offered by the Company.

The Company shall not disclose the data of its financial consumers and shall protect the confidentiality of its non-public consumer data. Consumer data shall only be utilized for the purposes specified and agreed with the financial consumer or as required under any applicable law.

This Policy is in addition to and does not replace or supersede any information in relation to the processing of personal data that is included in any of the existing Privacy Policy, Client Agreement, Partnership or Digital Affiliates Agreement. The Company's Privacy Policy, as amended from time to time, is published on the Company's website at exness.com and governs how the Company collects, uses, stores, discloses and transfers client's personal data and the individuals personal data rights during and after the termination of the business relationship.

3. Non-Public Data Collected and Processed

A list of non-public data collected and processed by the Company includes but is not limited to:

- Personal information such as: Name, surname, residential address, e-mail address, phone number, date of birth, gender, citizenship, occupation and employment details;
- Information for the construction of client's economic profile, including source of income and wealth, details about source of funds;
- Information on whether a client holds a prominent public function (PEPs);
- Bank Account and/or Credit card details or/and other payment details;
- Documents provided to the Company for verification of the client's identity i.e. passport/identity car, utility bills and other identifiable documents of clients who are physical persons;
- Documents provided to the Company for verification of identity of clients who are legal entities such as the legal entity's incorporation documents as applicable, financial statements, business plan, passport/ID, utility bills and other identifiable documents of directors, shareholders and authorized persons of the legal entity for verification purposes;
- Any other information designated as confidential.

4. Sensitive Data collected and/or processed

The Company considers the following personal data to be 'sensitive':

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- trade-union membership;
- genetic data, biometric data processed solely to identify a human being;
- health-related data;
- data concerning a person's sex life or sexual orientation.

The Company does not customarily collect and/or process sensitive data from clients or potential clients during the provision of the services. Where the Company will ask you for sensitive personal data it will always tell you why and how the information will be used.

5. The Purpose for which non-public consumer data is collected and used

The Non-public consumer data collected by the Company are used in all stages of its business relationship with consumers to be able to provide the services and products based on the client services agreement and business relationship with the clients. In other words, the Company needs to collect the data explained above for the performance of its contractual obligations towards clients. In addition, processing of personal data takes place to be able to complete our client due diligence and onboarding process, as well as to ensure the provision of high-quality services to its clients.

The Company is subject to several laws and regulations including anti-money laundering laws and financial services laws while it is under the supervision of competent authorities such as Financial Services Authority in Seychelles whose laws, regulations and circulars apply to the Company. For this purpose, the Company is required to comply and collect certain data during the client onboarding and ongoing monitoring of clients as well as

transactions and/or request information from clients for risk mitigation/management reasons.

At the beginning of the Company's – consumer relationship, non-public consumer data such as without limitation full name, address and telephone number are required by the Company to authenticate/verify the identity of a client. Identifying the true identity of a client is of crucial importance for the Company, as it enables the Company to identify, assess, mitigate, prevent and investigate possible fraudulent activity.

In the course of the Company's – consumer relationship, non-public consumer data such as without limitation the risk aversion, income and profession of a client are required by the Company to assess the appropriateness of the products and services it provides to consumers. In addition, using the consumer's data the company is able to manage the client's account and/or inform the client about any products or services that may be of his/her interest. Apart from the aforesaid, the data can be used by the Company for statistical purposes with the aim of improving its products and services as well as to update clients on any issues that might arise regarding their business relationship with the Company.

Lastly, non-public consumer data is necessary at the stage at which a client decides to terminate its relationship with the Company. In this stage, non-public consumer data might be used for the purpose of resolving and/or assessing the history of a client's complaint. It is noted that non-public consumer data is kept by the Company for a period of 7 years from the date of the client's last transaction with the Company, in line with AML and the requirements of our Regulatory Authority.

6. Security practices and procedures to safeguard non-public consumer data

The Company implements the required procedures for safeguarding the security, integrity, and confidentiality of information, considering the nature of the information to be stored.

Agents or third parties that assist the Company to provide its services to clients shall maintain the confidentiality of non-public consumer data and use such information only in the course of providing their services, based on the Company's directions.

The Company monitors the activities of agents and third parties acting on its behalf on the basis of the relevant agreements that are in place for each business relationship.

The security of non-public consumer data is of utmost importance for the Company. For this reason, the Company implements a number of procedures on the accessibility and protection of data.

Specifically, non-public consumer data is only accessible by employees who need the specific information in order to operate, develop or improve the Company's services. Such individuals are bound by confidentiality and are subject to internal disciplinary procedures in case they fail to meet their obligations.

The accessibility of non-public consumer information by employees is based on the following principles:

a. Differentiation of the access rights depending on job responsibilities
b. Protect systems using technical measures at the network, system and application levels, as well as organisational measures
c. Responsibility measures for the illegal rendering of the information to the employees of the Company and by individuals outside the Company
d. Ensure confidentiality of information by using data encryption and access control.

7. Collection of non-public consumer data

7.1. Processing of data

The processing of non-public consumer data is carried out through the information processing systems used by the Company. The data collected from consumers are only processed and analysed by the employees of the Company, and by persons who have the required authority and rights to use such data. The Company treats unauthorized access to data by employees as a serious violation of the Company's internal policies and procedures. To this end, any unauthorized access to non-public consumer data by employees is subject to disciplinary procedures, without prior notice.

The Client can request from the Company to restrict and/or terminate the processing of his/her Personal Data at any time and the Company shall duly consider such request based on the applicable laws and regulations.

7.2. Data Protection Officer

In accordance with local regulations, the Company has appointed a Data Protection Officer who will, among other duties:

- Monitoring compliance with the policies on the protection of personal data and compliance with the Data Protection Laws.
- Act as the contact point for the Commission on issues relating to processing, including consultation, investigations, audits or any other aspect that the Commission deems necessary in relation to the data protection laws.
- Act as the main focal point to the data subject's complaints, and shall be responsible for establishing adequate mechanisms to adopt handling of disputes.

7.3. Intended recipients

The intended recipients of non-public consumer data shall be the employees of the Company, persons who possess the required rights and authority to access such data. In addition, any agent's or third parties acting on behalf of the Company should be considered as intended recipients of the data only in case such data is required in the course of providing their services, based on their agreement with the Company.

7.4 Non-public consumer data rights

The Client may exercise the following rights in relation to the non-public data the Company holds by sending an email at support@exness.com.

- Right to review

Every financial consumer has the right to review his/her non-public consumer data stored by the Company, upon request to the Company.

- Right to correct or amend

Every financial consumer has the right to correct or amend his/her non-public consumer data stored by the Company, upon request to the Company.

8. Storage of non-public consumer data

The Company undertakes all reasonable and appropriate organisational, physical and technical measures for the protection of non-public consumer data against unlawful access, destruction, misuse or accidental loss.

Non-public consumer data are being stored on the various databases of the Company located on the Company's server and cloud. For the purpose of protecting the stored data, the Company implements the procedures analysed in *Section 6* of this manual.

For safeguarding the Company's recorded data from possible loss, the Company implements consistent, reliable and documented back up procedures. The back up procedure is automatic and takes place in different ways and frequency depending on the criticality level of the relevant business application system.

The Company keeps client's non-public consumer data on record for a period of seven (7) years from the date of the last transaction of the client with the Company. In case there is an investigation against any customers the documents will be kept according to the instructions of the investigating authority.

The Company will be able to retrieve the relevant documents/data without undue delay and present them at any time to the local authorities if requested.

9. Disclosure of non-public consumer data

The Company may disclose non-public consumer data to a third party in the following circumstances:

a. If the client has been informed about the disclosure and he/she has consented in writing to the disclosure.

b. If the third party to which the data will be disclosed has been authorized by the client to obtain the data from the Company.
c. If the Company is required to disclose the non-public consumer data under mandated Credit Reporting or under any other law or by a court order.

9.1. Voluntary Disclosure

Apart from the above circumstances, the Company might disclose the consumer's non-public data to third parties, on the basis that the consumer has voluntarily consented to this Policy, as described in section 10 below.

10. Client Consent

At the stage of establishing a business relationship with the consumer, the Company obtains the consumer voluntary consent to this policy. Such consent is obtained before the offering of any services to the consumer.

The Company may obtain the consumer's consent electronically in the form of a general agreement through the acceptance of the client services agreement and/or consider clients who have received and agreed to this policy electronically as clients who have given their consent to the disclosure of their non-public consumer data.

11. Amendment to the Policy

The Company reserves the right to make changes to this Confidentiality Policy from time to time for any reason and the client will be notified of such changes by posting an updated version of this Confidentiality Policy on the website. The client is responsible for regularly reviewing this Confidentiality Policy and the use of this website after any such changes are published, shall constitute an agreement to such changes.

12. How to contact us

The Consumer can extend any questions or requests he/she might have in relation to his/her data stored by the Company by sending an email at support@exness.com.