ELIDI Securities Ltd (ex UGM Securities Ltd)

Privacy Policy

February 2024

Table of Contents

1. Introduction

ELIDI Securities Ltd (the "Company") is committed to protecting customers' privacy. This Privacy Policy describes what Personal Data we collect, use and process and how this information is used in the course of our business.

2. Customer data

The Company collects customer data for various reasons, which include:

a) The provision of investment and ancillary services,
b) To ensure compliance with the provisions of the Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007-2021,
c) To communicate with customers,
d) For marketing purposes,
e) To defend its legal rights,
f) For recruitment, employment and payroll, and
g) For any other purpose similar to or connected to the above or for any other purpose that the customer will provide Personal Data to us.

Customer's data include name, address, identification details, postal and business address, mobile phone number, email, profession, bank account details, social insurance number, tax identification number, certificate of clean-criminal record, certificate of non-bankruptcy and other relevant details. This data is stored and processed by the Company throughout the validity period of the contract / relationship, in order to provide the requested services, handle requests and/or enquiries and perform payments. This data is also stored for a period of five years after the termination of the contract / relationship.

3. Processing activity name

The Company may process the Personal Data set out above for any of the following purposes:

a) Disclose Personal Data to the Cyprus Securities and Exchange Commission and/or the Central Bank of Cyprus, as per the relevant legal requirements,
b) Disclose information that is essential to auditors, legal consultants, operational partners, support services partners and affiliates for the complete provision of the service to the customer,
c) Provide information to the customer's authorized representative,
d) For compliance with a legal obligation of the Company,
e) For the protection of the customer's vital interests,
f) For purposes of legitimate interests of the Company, such as legal actions against the customer, the detection and prevention of fraud and IT purposes (e.g., cyber-security, data loss prevention),

g) Reveal to regulatory authorities, competent governmental authorities and agencies (other than tax authorities), law enforcement agencies, intergovernmental or supranational bodies, and other third parties with the requisite authority to request such information,
h) Reveal information in response to criminal or civil legal process as requested by the competent courts of the relevant jurisdiction and as permitted under Cyprus Laws,
i) Provide information for statistical purposes that do not include personal identification information but are of rather aggregate nature.

The Company takes all necessary steps to safeguard the Confidentiality, Integrity and Availability of its systems and services, e.g., to protect against cybersecurity threats, fraud, etc. Personal data is stored by the Company for a period of five years (may be extended to 7 years if requested by the competent authority) after the termination of the contract / relationship. After the lapse of this period this data is erased.

The following data is not erased:
a) Data processed for the purposes of legitimate interest (e.g., an action against a customer), which are maintained until the legitimate purpose is completed.

4. General customers' rights according to European Regulation 2016/679 ("GDPR")

4.1 Right of access

Customers may be informed in more detail about the Personal Data processes of the Company by:

a) Visiting the offices of the Company, completing, and submitting the relevant application form, or
b) Requesting via email at info@elidi.capital the relevant application form and submitting the said via the same email address.

The right of access is subject to the provisions of the Cyprus data protection legislation and the authentication of the legal subscriber.

4.2 Right to erasure ("right to be forgotten")

Customers may request the erasure of any of their Personal Data by:

a) Visiting the offices of the Company, completing, and submitting the relevant application form, or
b) Requesting via email at info@elidi.capital the relevant application form and submitting the said via the same email address.

The right to erasure is subject to the provisions of the Cyprus data protection legislation and the authentication of the legal subscriber.

4.3 Data portability

Customers may exercise the right to data portability by:

a) Visiting the offices of the Company, completing, and submitting the relevant application form, or
b) Requesting via email at info@elidi.capital the relevant application form and submitting the said via the same email address.

Data portability is subject to the provisions of the Cyprus data protection legislation and the authentication of the legal subscriber.

4.4 Right of updating, rectification, or minimization of Personal Data

Customers may update their Personal Data or request the correction of any inaccurate Personal Data or data minimization, by:

a) Visiting the offices of the Company, completing, and submitting the relevant application form, or
b) Requesting via email at info@elidi.capital the relevant application form and submitting the said via the same email address.

These rights are subject to the provisions of the Cyprus data protection legislation and the authentication of the legal subscriber.

5. Information security measures

The Company maintains solid information security measures and procedures to safeguard customers' Personal Data, in line with our legal obligations.

A comprehensive approach is considered for information security to effectively ensure the Confidentiality, Integrity and Availability of customers' Personal Data. The Company endeavors to implement a holistic Information Security Management System to effectively safeguard the Confidentiality, Integrity and Availability of our Customers data.

6. Transfers outside the EU/EEA

Customers are informed that the associates of the Company are based both within the EU and/or the EEA but also outside the EU and/or the EEA. Partners within the EU/EAA are contractually committed to the Company to provide appropriate security safeguards and to maintain the confidentiality of the customers' Personal Data. With regards to Personal Data shared outside the EU/EEA and subsequently accessed by other entities,

these shall only be shared when there are guarantees of an adequate level of protection in terms of applicable law and remain limited to the minimum necessary for the intended purposes, on the condition that all relevant data protection agreements ("DPA") are in place and duly signed by the parties.

7. Contact information and complaints

Customers can contact the Company for any information on its Privacy Policy by phone at +357 22523603, or by post at A.G. Leventi 5, 9th Floor, Flat/Office 901, 1097 Nicosia, Cyprus, or by email at info@elidi.capital . The same contact details may be used for any inquiry or complaint.

The Company has NOT appointed a Data Protection Officer's ("DPO"). The duties of the DPO are assigned to the Compliance officer.

8. Data subject request policy

8.1 Data subject rights

The Company's employees may collect, store or process Personal Data in the course of their employment with the organization. Every employee has responsibilities under legislation to protect the rights of the individuals whose Personal Data the Company obtains, stores or processes ("Data Subjects"). Data Subjects for whom the Company obtains Personal Data have the following rights:

- to have their Personal Data obtained and processed fairly,
- to have Personal Data kept securely and not illegitimately disclosed to others,
- to be informed of the identity of the Data Controller and of the purpose for which the information is held,
- to get a copy of their Personal Data,
- to have their Personal Data corrected or deleted, and
- to prevent their Personal Data from being used for certain purposes, etc.

In accordance with Data Subject rights, the Company may receive a number of requests from Data Subjects. This policy provides details of what the Data Subject is entitled to and what the Company should do to comply with their statutory obligations.

8.2 Request for rectification of Personal Data held by the Company

Under Article 16 of the GDPR, Data Subjects have a right to the rectification of any inaccurate or incomplete Personal Data which is held by the Company. The Data Subject has the right to have incomplete Personal Data completed. The rectification of inaccurate or incomplete Personal Data held by the Company must be completed within 30 days of receipt of the request.

8.3 Request for erasure of Personal Data held by the Company (right to be forgotten)

Under Article 17 of the GDPR, Data Subjects have a right to the erasure of any Personal Data which is held by the Company where one of the following conditions applies:

a) The Personal Data are no longer necessary in relation to the purposes for which they were collected,
b) The Data Subject withdraws consent (this applies only where the Company is relying on consent only as a lawful basis to process the data),
c) The Data Subject objects to the Processing and there are no overriding legitimate grounds for the Processing, or the data subject objects to the Processing for direct marketing purposes,
d) The Personal Data has been unlawfully processed,
e) The Personal Data have to be erased for compliance with a legal obligation to which the Company is subject.

Where a request is made for the erasure of Personal Data held by the Company and one of the above conditions applies, the request must be complied with within 30 days of receipt of the request.

8.4 Data Subject access requests

Under Article 15 of the GDPR, Data Subjects have a right of access to their Personal Data which is held by the Company. A Data Subject also has a right to obtain confirmation from the Company as to whether or not Personal Data concerning him or her is being processed by the Company. A charge cannot be levied on the Data Subject for the provision of this information.

When a Data Subject access request is received by the Company, the employee/s who receive/s the correspondence will refer it directly to the Compliance Officer. In the event that the Data Subject is not known to the Compliance Officer or the information management team, a response requesting proof of identification should be issued without undue delay.

The relevant department(s) and the relevant individuals within those departments who have processed Personal Data belonging to the Data Subject will be identified. Searches will be conducted by the relevant individuals for the requested data both electronically and manually. The Compliance Officer will request the relevant individuals to provide an accurate estimate of the volume of data held and an estimate of the time that it would take to carry out a thorough review of the documentation. In the event that searches reveal a volume of Personal Data that is incapable of being provided within 30 days, a response will be issued to the Data Subject requesting further detail on the information they require and asking the Data Subject to narrow the request where possible. In the event that the Data Subject does not narrow the request and the Compliance officer is satisfied that it will not be possible to comply with the request within 30 days, he/she

must respond to the Data Subject providing a breakdown of the reasons why it will not be possible to provide the information within the prescribed period.

All Personal Data must be provided to the Data Subject in a reasonable time within the prescribed period).

8.5 Information the Data Subject is entitled to in a response to a request

The Data Subject is entitled to receive confirmation within 30 days of the receipt of the request as to whether or not Personal Data concerning him or her are being processed, and, where that is the case, access to the Personal Data and the following information:

- the purposes of the Processing,
- the categories of Personal Data concerned,
- the recipients or categories of recipient to whom the Personal Data have been or will be disclosed, in particular recipients in third countries or international organizations,
- where possible, the retention period for the Personal Data,
- the existence of the right to request from the Controller rectification or erasure of Personal Data or restriction of Processing of Personal Data concerning the Data Subject or to object to such Processing,
- the right to lodge a complaint,
- where the Personal Data are not collected from the Data Subject, any available information as to their source,
- the existence of automated decision-making (if applicable), including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

Employees must bring all Data Subject access requests to the attention of the Compliance Officer immediately. Failure to do so may result in disciplinary action.

8.6 Roles and responsibilities of the Company

The Company has overall responsibility for ensuring compliance with the GDPR. However, all employees of the Company who collect and/or control the contents and use of Personal Data are also responsible for compliance with the GDPR.

The Company will provide support, assistance, advice and training to all relevant departments, officers and staff to ensure it is in a position to comply with the GDPR.

Contact Person:
Compliance officer
info@elidi.capital.

9. Definitions

“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.

“Personal Data”: means any information relating to an identified or identifiable natural person. 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, organization, 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.