KPMG Center, Level 2
1 Agias Fylaxeos Street,
3025 Limassol, Cyprus

PRIVACY POLICY

1. Introduction

VPR Safe Financial Group Ltd (hereinafter the "Company") is incorporated under the laws of the Republic of Cyprus with Registration No. HE 322134. The Company is authorized and regulated by the Cyprus Securities and Exchange Commission ("CySEC") as a Cyprus Investment Firm ("CIF"), with license number 236/14 to provide certain Investment Services under the Provision of Investment Services, the Exercise of Investment Activities, the Operation of Regulated Markets and Other Related Matters Law of 2017, Law 87(I)/2017 (hereinafter the "Law").

1.1 This Privacy Policy ((herein the "Policy") sets out the Company's obligation regarding the collection, processing, transfer, storage and disposal of personal data relating to existing and prospective Clients as well as to any visitors or users of the Company's website(s), and other third parties (hereinafter the "Data Subjects" and/or "Clients") in accordance with the General Data Protection Regulation (Regulation (EU) 2016/679) (hereinafter "GDPR"),

1.2 The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

1.3 The Company is committed to protect the privacy of all Data Subjects' personal data. The Company would like to assure any existing or prospective Clients, applicants, users and visitors that it has taken measurable steps to protect the confidentiality, security and integrity of the their information.

1.4 The Company controls the ways the Data Subjects' Personal Data is collected and the purposes for which the Data Subject's Personal Data is used by the Company, acting as the "data controller" for the purposes of applicable European data protection legislation.

1.5 "Data 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

1.6 "Personal Data" means any information relating to an identified or identifiable natural person.

2. Collection of Personal Data

When you create an account with the Company, we require you to provide your first and last name, e-mail address, details about your financial status, your residential address, phone number, date of birth, a copy of a document to verify your identity (e.g. your national identity card or passport or driving licence), a copy

of a recent utility bill/bank statement (or similar) as evidence of your residential address, credit card or bank card details, Tax residence and Tax Identification Number, profession and employment details, knowledge and experience in trading, risk tolerance and risk profile and other information we may consider necessary to our functions and activities and in order to be in a position and be permitted to provide our services to you.

If the Company requests you to provide personal data and you fail to do so the Company may not be in a position to provide a service and/or enter into an agreement with you, in which case it will inform you accordingly.

The abovementioned data are collected by the Company when you are going to open a trading account with the Company. It is required by the AML Law (the Prevention and Suppression of Money laundering and Terrorist Financing Law of 2007 L. 188(I)/2007-2018 as amended from time to time) and CySEC's AML Directive that the Company collects the necessary data for verifying your identity, constructing your economic profile, monitoring your account and verifying the source of funds (when it is necessary). Additionally, we use this data to set up and administer your trading account, provide technical and customer support.

If you are a corporate Client we are required to collect information related to the legal entity (e.g. corporate and constitutional documents), additional personal information on the shareholders, directors and other officers that we deem as necessary in order to be compliant with our legal and regulatory requirements.

We may record any communications, electronic, by telephone, in person or otherwise, that we have with you in relation to the services we provide to you and our relationship with you. These recordings will be our sole property and will constitute evidence of the communications between us. It should be note that we are obliged by the Law to keep records of all telephone conversations and electronic communications that are related to transactions concluded or intended to result in transactions when dealing on own account and the provision of Client order services that relate to the reception, transmission and execution of Client orders.

The Company may also collect the Client's Information in regards to their use of the Company's website(s), such as pages visited, frequency, duration of visit and trading activities. With regards to each of the Client's visits to the website, the Company may automatically collect information including internet protocol (IP) address, login information, browser type and version, time zone, phone numbers used to call their customer service number.

3. Use of Personal Data

3.1 The Company can only process Data Subjects' Personal Data when there is a genuine reason to do so and it must be one of the following:

a) To fulfil any contract the Company to which the Data Subject is a party or to take steps at the request of the Data Subject prior to entering a contract;
b) The Company is subject to a legal obligation;
c) Where the Data Subject has given consent to the Company to process his/her data;
d) When the processing is necessary for the purposes of legitimate interest pursued by the Company or a third party, except when such interests are overridden by the interests of fundamental rights and freedoms of the Data Subject;
e) When the 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 Company;
f) When it is in the Data Subject's vital interest or of another natural person.

3.2 The Company shall not be liable for misuse or loss of personal information and/or otherwise on website(s) the Company does not have access to or control over.

3.3 The Company will not be liable for unlawful or unauthorized use of the Data Subject's personal information due to misuse and/or misplacement and/or malicious use of the Data Subject's passwords, either by the Data Subject or any third party.

3.4 The Company will use, store, process and handle the Data Subject's Personal Information (in case they are a natural person or a legal representative) in accordance with the GDPR. The Company may be required to retain and use personal data to meet its' internal and external audit requirements, for data security purposes. Additionally the Company has the right to disclose Client information (including recordings and documents of a confidential nature, card details) in the following circumstances:
a) To comply with the Company's obligations under the GDPR, this Policy and the Company's Terms and Conditions, which may include laws and regulations outside the Data Subject's country of residence;
b) To respond to requests from courts, law enforcement agencies, regulatory agencies, and other public and government authorities, which may include such authorities outside the Data Subject's country of residence;
c) To monitor compliance with and enforce the Company's Platform terms and conditions;
d) To carry out anti-money laundering, sanctions or Know Your Customer checks as per CySEC's AML Directive and MiFID II laws and regulations; or
e) To protect the Company's rights, privacy, safety, property, or those of other persons. The Company may also be required to use and retain personal data after the Data Subject has closed the Data Subject's account for legal, regulatory and compliance reasons, such as the prevention, detection or investigation of a crime; loss prevention; or fraud prevention.
f) to such an extent as reasonably required so as to execute Orders and for purposes ancillary to the provision of the Services;
g) to payment service providers and banks processing your transactions;
h) to auditors or contractors or other advisers auditing, assisting with or advising on any of our business purposes; provided that in each case the relevant professional shall be informed about

the confidential nature of such information and commit to the confidentiality herein obligations as well;

i) only to the extent required and only the contact details to other service providers who create, maintain or process databases (whether electronic or not), offer record keeping services, email transmission services, messaging services or similar services which aim to assist the Company collect, storage, process and use Client information or get in touch with the Client or improve the provision of the Services under this Agreement.

j) to a Trade Repository or similar under the Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties (CCPs) and trade repositories (TRs) (EMIR).

k) only to the extent required, to other service providers for statistical purposes in order to improve the Company's marketing, in such a case the data will be provided in an aggregate form.

l) only to the extent required, to market research call centers that provide telephone or email surveys with the purpose to improve the services of the Company, in such a case only the contact details will be provided.

m) to anyone authorized by you

n) to an Affiliate or introducing broker of the Company or any other company in the same group of the Company.

o) to any third-party where such disclosure is required in order to provide investment and ancillary services and enforce or apply our Terms and Conditions or other relevant agreements.

p) to successors or assignees or transferees or buyers, with ten Business Days prior Written Notice to the Client; this will happen in the event that the Company decides to sell, transfer, assign or novate to a third party any or all of its rights, benefits or obligations under the Agreement with you or the performance of the entire Agreement subject to providing 15 Business Days Prior Written Notice to the Client. This may be done without limitation in the event of merger or acquisition of the Company with a third party, reorganization of the Company, winding up of the Company or sale or transfer of all or part of the business or the assets of the Company to a third party.

q) Client Information is disclosed in relation to US taxpayers to the Inland Revenue in Cyprus, which will in turn report this information to the IRS of the US according to the Foreign Account Tax Compliance Act (FATCA) of the USA and the relevant intergovernmental agreement between Cyprus and the US.

3.5 The Company also collects and processes non-personal, anonymized data for statistical purposes and analysis and to help the Company in providing its Data Subjects with better products and services in the future.

3.6 Data Subjects' information which the Company holds is to be treated by the Company as confidential and will not be used for any purpose other than those stated above.

4. Legitimate Interests

4.1 When the Company has a business or commercial reason to process the Client's Personal Data this is referred to as a legitimate interest. The Clients Personal Data is still protected and the Company will not process data in a way that would be unfair to the Client and his/her interests.

4.2 If the Company does use legitimate interests as a reason to process Clients Personal Data the Company will advise the Client, what the Company's legitimate interests are and provide the Client with a method to raise any questions or objections they may have. However, compelling grounds for processing such information may over-ride the Client's right to object.

5. Data Subject Records

5.1 Whenever the Data Subject's data is kept by the Company, the Company will ensure that it is appropriately protected and only used for acceptable purposes, as stated above.

5.2 Under the applicable regulatory obligations, the Company is required to retain copies and evidence of the actions taken by us in regard to your identity verification, sources of incomes and wealth, monitoring of your transactions, telephone, chat and email communications, orders and trades history, handling of your complaints and records that can demonstrate that we have acted in line with regulatory code of conduct throughout the business relationship. These records must be maintained for a period of **at least 5 (five) years and/or up to a maximum of 7 (seven) years** after the termination of the business. The Client's Personal Data may be kept longer if the Company cannot delete it for technical reasons. When we no longer need personal data, we securely delete or destroy it.

6. Contacting the Data Subject

6.1 The Company may, for the purpose of administering the terms of the Client Agreement, from time to time, make direct contact with the Client by telephone, SMS, fax, email, or post.

6.2 In accordance to the applicable laws and regulations and the GDPR, telephone calls to and from the Company may be recorded for training and security purposes along with the resolution of any queries arising from the service the Client receives. Any recordings will be the sole property of the Company.

6.3 If the Client agrees, the Company or any of their Affiliates or any other company in their group of Companies, may make contact with the Client from time to time, by telephone, SMS, fax, email or post for marketing purposes to bring to their attention products or services that may be of interest to the Client or to conduct market research.

7. Security of Personal Data

7.1 Depending on the Services the Client chooses, the Company may need to share the Client's Personal Data with the third parties that provide those services. Where the Client's Personal Data is transferred

outside of the European Economic Area ("EEA"), the Company requires that appropriate safeguards are in place. Please see section 9 further below.

7.2 The personal information the Data Subject provides in connection with registering themselves as users of the website or of the Company's services is classified as 'Registered Information'. The Company offers high protection of the Registration Information provided by the Data Subject. The Data Subject can access their "Registered Information" through a username and password selected by them. It is their responsibility to ensure that their password is encrypted and known only to them. "Registered Information" is safely stored on secure servers and is only accessible by authorized personnel via a username and password. The Company encrypts all personal information as it is transferred to them and thus makes all necessary effort to prevent unauthorized users from viewing any such information. Personal information provided to the Company that is not 'Registered Information' also resides on secure servers and is again accessible only by authorized personnel via password.

7.3 The Company takes the appropriate measures to ensure a level of security appropriate to protect any personal data provided to us from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

7.4 The Company implements appropriate technical and organisational measures such as data encryption, access management procedure, clean desk policy, business continuity and disaster recovery, IT systems risk assessment, physical and logical access segregation, process in case of personal data breach policy etc. Additionally, the Company limits access to the Client's personal data to those employees, agents, contractors and other third parties who need to know. They will only process the Client's personal data on the Company's instructions and they are subject to a duty of confidentiality.

Your personal data may be stored electronically or in paper form.

8. Confidentiality Obligations

8.1 The Data Subject's Information (not in the public domain or already possessed by the Company without a duty of confidentiality) which the Company holds, is to be treated as confidential and will not be used for any purpose other than in connection with the provision, administration and improvement of their Services to the Data Subject or the furthering of the Data Subject Agreement, for managing the Data Subject's account, for reviewing their ongoing needs, for enhancing customer service and products, for giving the Data Subject ongoing information or opportunities the Company believes may be relevant to the Data Subject, for improving their business relationship, for anti-money laundering and due diligence checks, for research and statistical purposes and for marketing purposes.

9. Data Transfer outside the EEA

When the Company transfers your data to other third parties outside the EEA such transfers will comply with the General Data Protection Regulation (Regulation EU 2016/679, and hence the Company may in

some cases rely on a Commission Adequacy decision, or appropriate safeguards (e.g. applicable standard contractual clauses, binding corporate rules, the EU-US Privacy Shield or any other equivalent applicable arrangements) or other grounds provided by the GDPR.

You may contact the Company in order to be informed of the appropriate or suitable safeguards.

10. Right of Access & Data Subject's rights over their Personal Data

Under the GDPR, Data Subjects have the following rights:

10.1 **Right of access –** you have the right to request from us to provide you with a copy of the personal data that we hold about you.

The Company will give the Data Subject access to their personal data (including a copy or the ability to send the data to another provider) on request unless any relevant legal requirements prevent them from doing so or other exemptions apply. Before providing access to the Data Subject, the Company will ask him/her to prove their identity and give sufficient information about themselves.

10.2 **Right of rectification** – you have a right to request from us to correct the personal data that we hold about you that is inaccurate or incomplete.

10.3 **Right to be forgotten** – you have a right to request from us in certain circumstances to erase your personal data from our records. In case that these circumstances apply to your case and provided that no exception to this obligation applies (e.g. where we are obliged to store your personal data in compliance with a legal obligation under Cypriot or EU law), the Company acting as your controller will erase your personal data from its records.

If the Data Subject requests the deletion of their personal data, this will result in the automatic closure of their account and the Company will remove their personal data from active processing. However, as in accordance to applicable laws and regulations the Company will be required to maintain the Data Subject's personal data to comply with their legal and regulatory requirements as well as in accordance with their internal compliance requirements in relation to maintaining records.

10.4 **Right to restriction of processing** – you have a right to request from us where certain conditions apply, to restrict the processing of your personal data.

10.5 **Right of portability** – you have the right to request from us where certain conditions apply, to have the data we hold about you transferred to another organisation. Where these conditions apply the Company will transfer your personal data to another organisation.

10.6 **Right to object** – you have the right to object on grounds relating to your particular situation, to certain types of processing such as direct marketing or where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

10.7 **Request the transfer of your personal data to you or to a third party** - We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

10.8 **Right to withdraw consent where we are relying on consent to process your personal data** - However, this will not affect the lawfulness of any processing carried out before you withdraw services to you. We will advise you if this is the case at the time you withdraw your consent

The Data Subject may contact the Company via e-mail at compliance@alvexo.com

The Data Subject is not obliged to provide the Company with any personal data. In the absence of this information however, the Company may not be able to open an account for the Data Subject and/or to provide the Data Subject with any other services, information or assistance.

11. Automated decision – making and profiling

In order to perform the contact between us and as required by the Law and the relevant Circulars issued by CySEC, it is requested for the provision of the investment services to you, to assess your knowledge and experience, your financial situation and investment objectives.

We will fulfil the above requirements through the following tools.

Appropriateness Test: it takes place when you require registering as client of the Company. Hence, we need to check and ensure that you are suitable for the provision of the Company's services and products by taking an appropriateness test in regards to your knowledge, financial background and experience in regards to financial services. Based on the scoring you receive, you will be informed whether you are eligible to receive our services and become our Client and the maximum level of leverage you are eligible to, as applicable. The reason for assessing your appropriateness is to enable the Company to offer to you services suitable to you and act in the client's best interest.

The scorings above are monitored by the Compliance department of the Company. During these processes, the Company takes all the technical and operational measures to correct inaccuracies and minimize the risk of errors, to prevent any discrimination and to secure personal data of the client.

KPMG Center, Level 2
1 Agias Fylaxeos Street,
3025 Limassol, Cyprus

12. Cookies

12.1 The Company uses cookies to store and collect information about how Data Subjects use the Company's website. Cookies are small text files stored by the browser on the Data Subject's equipment's hard drive. They send information stored on them back to the Company's web server when the Data Subject accesses the Website. These cookies enable the Company to put in place personal settings and load the Data Subjects' personal preferences to improve their experience. Information about cookies is included in the Company's "Cookies Policy" available on our Website.

13. Contact us or making a complaint

13.1 If the Data Subject has any questions regarding this policy, wish to exercise any of their rights or have a complaint or if they have any questions about security on the Website, they may email the Company at **compliance@alvexo.com** and thereafter, the request shall be forwarded to the Company's Data Protection Officer, as applicable.

13.2 We try to respond to your request within one month. In case that your request takes us longer than one month we will notify you accordingly and keep you updated. In this respect it should be noted that the information to be provided as a result of exercising your right shall be provided free of charge. Nonetheless and where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the Company may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request

If you are not satisfied with our response to your complaint and/or your request was not handled within the timeframes specified, you have the right to lodge a complaint with our supervisory authority, the Cyprus Data Protection Commissioner. Alternatively, you also have the right to lodge a complaint with the data protection authority of your country of residence.

You can find information about how to contact the Cyprus Data Protection Commissioner on the following website: http://www.dataprotection.gov.cy

14. Update of this Policy

We may make changes to this Policy from time to time and it is important that you check this Policy for any updates. Any personal information we hold will be governed by our most current Privacy Policy. If we make changes we consider to be important, we will communicate them to you.