

PRIVACY POLICY

1. Introduction

- 1.1 VPR Safe Financial Group Ltd (hereinafter the “Company”) is incorporate 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 2007, Law 144(I)/2007, as subsequently amended or replaced from time to time (“the Law”).
- 1.2 The Company acting in its capacity as a CIF and in accordance with the provisions of the Law, outlines in the Privacy Policy (herein the “Policy”) how the Company collects, maintains, uses and discloses personal information of the Client.
- 1.3 This Policy applies to existing and prospective Clients as well as to any visitors of the Company’s website (s).
- 1.4 The Company is committed to protecting the privacy of all Client’s personal data which it obtains during the Account Opening process, including but not limited to, information obtained during a Client’s visit to the Company/s websites. The Company would like to assure any existing or prospective clients, applicants and visitors that it has taken measurable steps to protect the confidentiality, security and integrity of the Client’s Information.
- 1.5 The Company controls the ways the Client’s Personal Data is collected and the purposes for which the Client’s Personal Data is used by the Company, acting as the “data controller” for the purposes of applicable European data protection legislation.

2. Collection of Personal Data

- 2.1 The Company will use the Client’s Personal Data only in accordance with Directive 95/46/EC on the Protection of Personal Data, the Processing of Personal Data (Protection of the Individual) Law 138(I)/2001, the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) Law, this Policy and the Company’s Terms and Conditions. The Company can only process Clients’ 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 may have with Data Subject (“the Client”)
 - b) The Company has have a legal obligation
 - c) Where the client has given consent to the Company to process his/her data
 - d) When it is in the Company’s legitimate interest
 - e) When it is in the public interest
 - f) When it is in the Client’s vital interest
- 2.2 In order to open an account with the Company, the Client must first complete the online application form found on the Company’s website(s), accept and submit the online application form to the

Company and provide all the required documents. By completing the application form, private information is requested in order to enable the Company to evaluate the Client's application and comply with the applicable laws and regulations governing the provision of financial services. This information shall be used by the Company in order to contact the Client for information regarding the services offered by the Company.

2.3 Personal data collected includes but is not limited to:

- Personal details such as name, address, telephone number and/or e-mail address;
- Financial details such as estimated annual income and net worth, trading experience and investment knowledge;
- Identity verification Documents such as passport and Identity Card, Driver's License, Utility Bills, and/or bank statements or company information/corporate documents in case of an entity.

3. Use of Personal Data

3.1 The Company will use, store, process and handle the Client's Personal Information (in case they are a natural person) in connection with the furthering of the Agreement between the Company and the Client, in accordance to the Personal Data (Protection of the Individual) Law 138(I)/2001, the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) Law as amended or replaced from time to time. The Company may be required to retain and use personal data to meet the Client's internal and external audit requirements, for data security purposes and as believed to be necessary or appropriate in order:

- a) To comply with the Company's obligations under Directive 95/46/EC on the Protection of Personal Data, the Processing of Personal Data (Protection of the Individual) Law 138(I)/2001, the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) Law, this Policy and the Company's Terms and Condition, which may include laws and regulations outside the Client'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 Client'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 Directive DI144-2007-08 OF 2012 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 Client has closed the Client's account for legal, regulatory and compliance reasons, such as the prevention, detection or investigation of a crime; loss prevention; or fraud prevention.

3.2 The Company also collect and process non-personal, anonymised data for statistical purposes and analysis and to help the Company in providing its Clients with better products and services in the future.

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 Client's 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 Client's 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. Client Records

- 5.1 Whenever the Client's data is kept by the Company, the Company will ensure that it is appropriately protected and only used for acceptable purposes.
- 5.2 Under the regulatory obligations as per MiFID II Regulations, Directive 2014/65/EU, the Company is required to keep records containing Client personal data, trading information, account opening documents, communications and any other information which relate to the Client after the execution of each transaction for at least 5 (five) years and/or up to a maximum of 7 (seven) years after the termination of the business relationship. The Client's Personal Data may be kept longer if the Company cannot delete it for technical reasons.

6. Payment Gateway Providers

The Company uses payment gateway providers to enable its Clients to deposit and withdraw funds securely to and from a Client's account. Payment Gateway Providers do not retain, share, store or use the Client's personal information or any other purposes other than to allow the Client to deposit and/or withdraw from his/her account.

7. Contacting the Client

- 7.1 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.
In accordance to MiFID II regulations and the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) Law, 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 and recordings will be the sole property of the Company.
- 7.2 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.

8. Processing of Personal Data

8.1 The purpose of data processing may only be changed with the consent of the client or to the extent permitted by the national law to which the participating company transferring the data is subject. The Company reserves the right to process personal information obtained from the Client if:

- a) The Client has freely given his/her unambiguous, effective consent;
- b) Such action is required by applicable laws and/or by any competent authority having power over the Company;
- c) Data processing is for the purpose of establishing a contractual relationship or similar relationship of trust with the Client; or
- d) Processing is necessary to safeguard justified interests of the Company and/or any other third party to which such information is supplied and there are no grounds for assuming that the client has an overriding legitimate interest in precluding data processing;
- e) Such processing is necessary to protect the rights of the Company;
- f) Processing is necessary for compliance with a legal obligations imposed by law or to enforce legislation;
- g) For the conduct of proceeding in any court or tribunal that have commenced or are reasonably contemplated;
- h) Processing is required, exceptionally, to protect the life, health or safety of the Client.

In addition to the above, Affiliates or any other third party to which personal information is supplied to, ensure to provide simple, fast and efficient procedures that allow the Client to withdraw his/her consent at any time.

8.2 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.

8.3 The company will not be liable for unlawful or unauthorised use of the Client's personal information due to misuse and/or misplacement and/or malicious use of the Client's passwords, either by the Client or any third party.

9. Security of Personal Data

9.1 The Company may collect the Client's Information directly from the Client (in their completed Account Opening Application Form or via email) or from other persons including for example: credit reference agencies, fraud prevention agencies, banks, other financial institutions, third authentication service providers, third parties the Client permits the Company to share their data with, third parties necessary to provide products or services which the Client has requested and the providers of public registers. This information includes, but is not limited to, personal details such as name, address, date of birth,



contact details, payment details, including credit card, debit card and bank account details, and other necessary financial information.

- 9.2 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 are transferred outside of the European Economic Area ("EEA"), the Company requires that appropriate safeguards are in place.
- 9.3 The Company may also disclose personal information to other companies within associated or subsidiary companies and to business partners, or successors in title to the Company's business.
- 9.4 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.
- 9.5 From time to time the Company may also request further information to help improve the Company's Service to the Client or the Company's activities (for the Providers of Trading Data) under the Company's relevant Agreement, as the case may be, or comply with Applicable Regulations.
- 9.6 The personal information the Client 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 Client. The Client 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 authorised 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 unauthorised parties 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 authorised personnel via password.
- 9.7 Transmission of information via the internet is not always completely secure; the Company will exercise all endeavors to protect the Client's personal data, yet they cannot guarantee the security of the data transmitted; any transmission is at the Client's own risk. Once the Company has received the Client's information they will use procedures and security features to try to prevent unauthorised access. Furthermore, the data the Company collects from the Client may be transferred to, and stored at, a destination outside the EEA. It may also be processed by staff operating outside the EEA who work for the Company or for one of the Company's suppliers. Such staff maybe engaged in, among other things, the fulfilment of the Client's order, the processing of their payment details and the provision of support services. By submitting their personal data, the Client agrees to this transfer, storing and

processing. The Company will take all steps reasonably necessary to ensure that the Client's data is treated securely and in accordance with this Privacy Policy.

10. Confidentiality Obligations

- 10.1 The Client'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 Client or the furthering of the Client Agreement, for managing the Client's account, for reviewing their ongoing needs, for enhancing customer service and products, for giving the Client ongoing information or opportunities the Company believes may be relevant to the Client, for improving their business relationship, for anti-money laundering and due diligence checks, for research and statistical purposes and for marketing purposes.
- 10.2 Under the Client Agreement, the Client agrees that the Company has the right to disclose Client information (including but not limited to, recordings and documents of a confidential nature, card details and personal details) in the following circumstances:
- a) Where required by law or a court order by a competent Court.
 - b) Where requested by CySEC or any other regulatory authority having control or jurisdiction over the Company or the Client or their associates or in whose territory the Company has Clients.
 - c) To relevant authorities to investigate or prevent fraud, money laundering or other illegal activity.
 - d) To such an extent as reasonably required so as to execute Orders and for purposes ancillary to the provision of the Services.
 - e) Third authentication service providers, banks and other financial institutions for credit checking, fraud prevention, anti-money laundering purposes, identification or due diligence checks of the Client. To do so they may check the details the Client supplied against any particulars on any database (public or otherwise) to which they have access. They may also use Client details in the future to assist other companies for verification purposes. A record of the search will be retained by the Company.
 - f) To the Company's professional advisors 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.
 - g) 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.
 - h) To a Trade Repository or similar under Regulation 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).
 - i) 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.

- j) 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 the data will be provided.
- k) Where necessary in order for the Company to defend or exercise its legal rights to any court or tribunal or arbitrator or Ombudsman or governmental authority.
- l) At the Client's request or with the Client's consent.
- m) To an Affiliate of the Company or any other company in the same group of the Company.
- n) To successors or assignees or transferees or buyers, with ten Business Days prior Written Notice to the Client.

Under such circumstances, the Company shall expressly inform the third party regarding the confidential nature of the information.

11. Data Transfer outside the EEA

11.1 The Client hereby acknowledges and understands that the Company may transfer personal information to a third party who is in a foreign country outside the Republic if:

- a) The Client has given their explicit consent to the proposed transfer, or
- b) The transfer is necessary for the performance of a contract between the Client and the Company or the implementation of pre- contractual measures taken in response to the Client's request;
- c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Client between the Company and the third party; or
- d) The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or
- e) The transfer is necessary for the protection of vital interests of the Client; or
- f) The transfer is for the benefit of the Client.

11.2 If the Company does transfer the Client's Personal Data outside of the EEA, within the group or to their business partners, they will take measures to ensure it is protected to the same standards as it would be within the EEA by relying on one of the following:

- a) The country that is receiving the Client's Personal Data has been found by the European Commission to offer the same level of protection as the EEA. More information can be found on the European Commission Justice website.
- b) The Company will use contracts that require the recipient to protect the Client's Personal Data to the same standards as it would be within the EEA.
- c) Where the transfer is to the USA and the recipient is registered with Privacy Shield. Privacy Shield is a framework that ensures Personal Data is protected to a level approved by the EU. Read more about Privacy Shield on the European Commission Justice website.

In some instances the Company may be compelled by law to disclose the Client's Personal Data to a third party and may have limited control over how it is protected by that party.

12. Safeguard Measures

- 12.1 The Client's Information is stored on secure servers.
- 12.2 The Company limits access of Client's Information only to authorized personnel or partners that need to know the information in order to enable the carrying out of the Client Agreement.
- 12.3 The Company has procedures in place regarding how to safeguard and use Client's Information, for example, by requesting the Company's Affiliates and employees to maintain the confidentiality of the Client's Information.
- 12.4 Following MiFID II Regulations, Directive 2014/65/EU, the Company will not keep the Client's Information for any longer than is required.
- 12.5 In many cases, information must be kept for considerable periods of time. As in accordance to MiFID II Regulations, Directive 2014/65/EU, retention periods will be determined taking into account the type of information that is collected and the purpose for which it is collected, bearing in mind the requirements applicable to the situation and the need to destroy outdated, unused information at the earliest reasonable time. Under the applicable MiFID II regulations, the Company will keep records containing Client personal data, trading information, account opening documents, communications and anything else which relates to the Client for at least 5 (five) years and or up to a maximum of 7 (seven) years after termination of the Agreement between the Company and the Client. In any event, the Company will keep the Client's Information for the duration of applicable Limitation of Actions Laws as a minimum.
- 12.6 The Company is committed to safeguarding and protecting personal data and will implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to protect any personal data provided to them from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

13. Change of Information

Under the Personal Data (Protection of the Individual) Law 138(I)/2001, the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) Law, the Company respects the Client's right to access and control their personal data. The Company will respond to requests for personal data and, where applicable, will correct, amend or delete the Client's personal data.

- a) Access to personal data: The Company will give the Client 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 Client, the Company will ask them to prove their identity and give sufficient information about them.

- b) Correction and deletion: The Client has the right to correct or amend their personal data if it is inaccurate or requires updating. They may also have the right to request for the deletion of their personal data. If the Client 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 MiFID II Regulations, Directive 2014/65/EU the Company will be required to maintain the Client'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.
- c) Restrict processing: If the Client would like to control the use of their information for marketing they may do it by contacting the company via email at compliance@alvexo.com

In certain circumstances the Client can ask the Company to stop processing their personal data. However, this may result in the Company being unable to continue to provide the Client access to the Platform.

14. Right of Access & Client's rights over their Personal Data

- 14.1 Under the Processing of Personal Data (Protection of the Individual) Law of 2001 and the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) Law, as amended or replaced from time to time, the Client, as a natural person, has the right to obtain a copy of any personal information which the Company holds about them and to advise the Company of any perceived inaccuracy.
- 14.2 To make a request, the Client may contact the Company, verifying their identity and specify the required information.
- 14.3 The Company will assist the Client if they choose to exercise any of their rights over their Personal Data, including:
 - a) Withdrawing their previously granted consent; however, this will not invalidate any previously consented processing
 - b) Lodging a complaint with any relevant Data Protection Authority
 - c) Access to the Client's Personal Data that the Company holds or processes
 - d) Correction of any Personal Data that is incorrect or out of date
 - e) Erasure of any Personal Data that the Company processes, subject to MiFID II Regulations, Directive 2014/65/EU
 - f) Restrict processing of the Client's Personal Data in certain circumstances
 - g) Asking the Company to provide the Client or another company they nominate with certain aspects of the Client's Personal Data, often referred to as 'the right to portability'
 - h) The ability to object to any processing data where the Company is doing it for their legitimate interests
 - i) The ability to contest a decision made entirely by automated processing, to express the Client's point of view and to request that a human review the decision

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

- 14.4 To The Client 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 Client and/or to provide the Client with any other services, information or assistance.

15. Cookies

- 15.1 Cookies are small text files stored on a user's computer for record-keeping purposes. The Company uses cookies on the Website. The Company does link the information that it stores in cookies to any personal information the Client submits while accessing the Company's website.
- 15.2 The Client will be able to review the Company's Cookie Policy to understand more about the kind of cookies they use and how they can control and delete cookies.

16. Contact us

- 16.1 If the Client has any questions regarding this policy, wish to access or change their information, have a complaint or if they have any questions about security on the Website, they may email the Company at compliance@alvexo.com
- 16.2 If the Client is not satisfied with the Company's response or believe they are not processing the Client's personal data in accordance with the law, they can escalate their complaint to the data protection regulator in their jurisdiction.

The Office of the Commissioner for Personal Data Protection, can be contacted at 1, Iasonos Street, 1082 Nicosia, Cyprus. Further information is available on the Office of the Commissioner for Personal Data Protection's website at <http://www.dataprotection.gov.cy>.

17. Update of this Policy

- 17.1 This Policy is subject to change without notice. For this reason the Client is advised to look for updates from time to time.