PRIOR CAPITAL

PRIVACY POLICY

Updated on

MAY 31, 2019

Risk Warning: CFDs are complex instruments and come with a high-risk of losing money rapidly due to leverage. 90.00% of retail investor accounts lose money when trading CFDs with this provider. You should consider whether you understand how CFDs work and whether you can afford to take the high-risk of losing your money. Please consider our Risk Disclosure.

PRIVACY POLICY

1.INTRODUCTION

At Prior Capital CY Ltd (former PriorFX Ltd) (hereinafter "**we**", "**us**" or "**our**" or the "**Company**") we are committed to protect our clients' privacy and handling their personal data in an open and transparent manner.

The purpose of this Privacy Policy (hereafter the "Policy") is to provide a clear explanation of when, why and how we collect and use personal data. We have designed it to be as user friendly as possible, and have separate it in sections to make it easy for you to find the information that is most relevant to you. We reserve the right to modify this Policy at our sole discretion, whenever we deem fit or appropriate, so please review this section frequently.

The new European Union (EU) Data Protection Law, the General Data Protection Regulation (GDPR), comes into effect on 25th of May 2018. The GDPR (EU) 2016/679 gives individuals in the EU more control over how their data is used and places certain obligations on businesses that process the information of those individuals. We have updated our Privacy Policy to reflect the new requirements of the GDPR.

2.WHO WE ARE

The Company is an Investment Firm authorized and regulated by the Cyprus Securities and Exchange Commission (hereafter the "CySEC") under the License No. CIF221/13. The head office of the Company is located at 196 Arch. Makarios III Ave., Ariel Corner, 3030 Limassol, Cyprus.

Prior Capital CY Ltd is incorporated and registered under the laws of the Republic of Cyprus under the certificate registration number HE321360 and operates in compliance with the European Markets in Financial Instruments Directive II (MiFID II) 2014/65/EU and the Cyprus Investment Services and Activities regulated Markets Law of 2017 (Law 87(I)/2017).

3. IDENTITY AND CONTACT DETAILS OF DATA CONTROLLER AND DATA PROTECTION OFFICER

A. Data Controller

In relation to GDPR the "data controller" means organisation which collects, determines the purposes and the way how any personal data is processed.

In relation to its former and perspective clients, counterparties and personnel the Company acts as data controller. The main establishment and the central administration of the Data Controller is situated at 196 Arch. Makarios III Ave., Ariel Corner, 3030 Limassol, Cyprus.

B. Data Protection Officer (DPO)

We have designated a Data Protection Officer (DPO), who is responsible to monitor compliance with this privacy policy as well as the applicable Laws and liaise with the Cyprus Supervisory Authority, namely the Office of the Commissioner for Personal Data Protection.

The DPO may be contacted directly with regards to all matters concerning this policy and the processing of your personal data including the enforcement of all applicable and available rights.

Official requests may be made by post at 196 Arch. Makarios III Ave., Ariel Corner, 3030 Limassol, Cyprus, or electronically at dpo@priorcapital.eu

4.HOW DO WE COLLECT PERSONAL DATA?

Being the regulated investment company, we collect, and process different types of personal data required by Anti-Money Laundering Law, the Cyprus Investment Services and Activities regulated Markets Law and other legislative requirements for the following purposes:

To establish business relationship with the Company including account opening, proper execution of trading and non-trading transactions.

We may also collect and process personal data which we lawfully obtain not only from our clients but also from third parties e.g. online screening tools such as World Check Compliance or any other. In relation to the client's transactions we are recording the telephone calls in line with applicable laws and regulations that we are subject to. In more limited circumstances, we also may collect images and video data via security cameras located at the entrance of our premises for security purposes in order to reduce the risk arising from unauthorised access, theft etc. The security cameras at the entrance have been positioned to avoid capturing the images of persons not visiting our premises. For this purpose, we have placed signs in our premises in all prominent places that are clearly visible and readable and convey appropriate information including our details, the purpose for using security cameras and our contact details.

5.WHAT CATEGORIES OF PERSONAL DATA DO WE COLLECT?

In relation to potential, historic and current clients we collect the following personal data:

CATEGORY	PERSONAL DATA
COMMUNICATION	• E-mail • Phone • Address • Skype • LiveChat
APPLICATION FOR ACCOUNT OPENING	• Name • Gender • Birth date • Occupation • PEPs (whether you hold/held a prominent public function) • Social Security Number • Employment status (employed/self-employ) • Tax registration (FATCA/CRS) • Assets and Income • Source of funds • Trading experience

	• Authentication data (e.g. signature)
VERIFICATION OF IDENTITY	• Passport / National ID / Driver's License
BUSINESS RELATIONSHIP	• Results of appropriateness and suitability test • AML risk profile • Banking details • Account balance • Trading activity • Record of your inquiries and our responses

6.WHAT LAWFUL REASONS DO WE HAVE FOR PROCESSING PERSONAL DATA?

In order to proceed with a business relationship our clients must provide their personal data to us which are necessary to operate our business and provide our products and services. This is a requirement under Anti-Money Laundering Law and the regulations of Cyprus Security and Exchange Commission (CySEC). The failure by our clients to provide us with their personal data will prevent us from commencing or continuing the business relationship.

In accordance with GDPR we may rely on the following lawful reasons when we collect and use personal data to operate our business and provide our products and services:

- Compliance with legal obligations– We may collect and process personal data in order to meet legal regulatory obligations such as Anti-Money Laundering Law and the regulations of Cyprus Security and Exchange Commission (CySEC) for anti-money laundering due diligence and quality control purposes including recording of business communications.
- Contract – We may process personal data in order to perform our contractual obligations as shown in our terms and conditions.
- Consent - We may rely on your freely given consent to keep and process personal data at the time you provided them to us for a purpose that does not relate to the above. You have the right to withdraw consent at any time. However, the Company is obliged to continue keeping and processing of Personal Data according to legislative requirements and would stop doing it only after expiration of time period required by relative law.
- Legitimate interests – We may rely on legitimate interests based on our evaluation that the processing is fair, reasonable and balanced. A legitimate interest is when we have a legal, business or commercial reason to use our clients' information. Instances of such processing activities can include, but not limited to initiating legal claims, preparing our defense in litigation procedures, initiating complaints to our regulator, operation of security cameras at the entrance for security purposes etc.

7.WHO DO WE SHARE YOUR PERSONAL DATA WITH?

In the course of our business relationship our clients' personal data may be provided to various departments within our Company.

In addition, the following third parties may also be the recipients of the personal data under the certain circumstances:

- Supervisory and other regulatory and public authorities, whereby a statutory obligation exists that we are subject to.
- Financial institutions and payment service providers within the European Economic Area (EEA) due to our contractual obligations to make payments to and receive deposits from Clients.
- Affiliates and other business partners through whom such Personal Data were collected for business purposes.

Third parties to whom we may disclose Personal Data may have their own privacy policies which describe how they use and protect Personal Data. If you want to learn more about their privacy practices, we encourage you to visit the websites of those third parties.

8.INTERNATIONAL TRANSFERS

We store Personal Data on servers located in the European Economic Area (EEA). We may transfer Personal Data to reputable third party organisations situated inside EEA when we have a business reason to engage these organisations. Each organisation is required to safeguard Personal Data in accordance with our contractual obligations and data protection legislation. We will always take steps to ensure that any international transfer of information is carefully managed to protect the client's rights and interests, in particular we will only transfer Clients' Personal Data to countries which are recognised as providing an adequate level of legal protection in accordance with GDPR.

You have the right to ask us for more information about the safeguards we have put in place as mentioned above. Contact us as set out in **Section 12** if you would like further information or to request a copy where the safeguard is documented (which may be redacted to ensure confidentiality).

9.WHAT ABOUT PERSONAL DATA SECURITY?

We have put appropriate technical and organisational measures including security policies and procedures in place to protect Personal Data from loss, misuse, alteration or destruction. We restrict access to information at our offices so that only officers and/or employees who need to know the information have access to it. Those individuals who have access to the data are required to maintain the confidentiality of such information. In addition, we have trained our employees on how to handle, manage and process personal data, applied upgraded technical measures and transformed our policies and procedures in a way that will comply with the GDPR.

We protect your information by using data security technology and using tools such as firewalls and data encryption. Images from security cameras are securely stored and only a limited number of authorised persons may have access to them.

We use Secure Socket Layer (SSL) encryption technology in order to protect certain information that you submit to us. This type of technology protects you from having your information intercepted by anyone other than us while it is being transmitted to us.

We work hard to ensure that our Website(s) is/are secure and meet(s) industry standards. We also use other safeguards such as firewalls, authentication systems (e.g., passwords and personal identification numbers),

and access control mechanisms to control unauthorized access to systems and data. We also require that you use your personal Access Codes (personal username and password) every time you access your account online. Please be aware that the transmission of data via the Internet is not completely secure. Whilst we do our best to try to protect the security of your Personal Data, we cannot ensure or guarantee the security of your data transmitted to our site; any transmission is at your own risk.

10.HOW LONG DO WE KEEP YOUR PERSONAL DATA?

We will keep our Clients' personal data for as long as we have a business relationship.

Once our business relationship has ended, we will hold your Personal Data on our systems for the longest of the following periods:

a) any retention period that is required by law or regulations (the Company shall keep your data for up to 5 (five) years from the date of your last activity on your account, unless legal or regulatory reasons prohibit us from destroying the data);

b) the end of the period in which litigation or investigations might arise in respect of the services; or

c) as directed by our own internal retention policies or practices, the length of which may vary depending on the nature of the information that is held.

The Personal Data processed for the purposes of sending newsletters shall be kept with us until you notify us that you no longer wish your Personal Data to be used for this purpose. Personal Data collected and processed through security cameras are overwritten securely within seven (7) days. The Personal Data processed for the purposes of sending newsletters shall be kept with us until you notify us that you no longer wish your Personal Data to be used for this purpose.

We maintain a data retention policy which we apply to records in our care. When your Personal Data is no longer required and we do not have a legal requirement to retain it, they will be securely destroyed.

11.DATA PROTECTION RIGHTS

Subject to the provisions of the GDPR, you have certain rights regarding the Personal Data we collect, process or disclose and that is related to you, including the right:

- To receive access to your Personal Data (right to access);
- To rectify inaccurate Personal Data concerning you (right to data rectification);
- To request deletion/ erasure of your Personal Data (right to erasure/deletion, "right to be forgotten");
- To receive the Personal Data provided by you in a structured, commonly used and machine-readable format and to transmit those Personal Data to another data controller (right to data portability);
- To object to the use of your Personal Data where such use is based on our legitimate interests or on public interests (right to object);
- In some cases, to request the restriction of processing of your Personal Data (right to restriction of processing);

- To withdraw the consent given to us with regard to the processing of your Personal Data at any time. Note that any withdrawal of consent will not affect the lawfulness of processing based on consent before it was withdrawn.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information or to exercise any of your other rights. This helps us to ensure that Personal Data is not disclosed to any person who has no right to receive it. No fee is required to make a request unless your request is clearly unfounded or excessive. Depending on the circumstances, we may be unable to comply with your request based on other lawful grounds, We will try to respond to all legitimate requests within one (1) month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

12.CONTACT AND COMPLAINTS

To exercise any of the above rights, or for any questions or complaints about our use of your Personal Data, please contact our Data Protection Officer (DPO), either by post at 196 Arch. Makarios III Ave., Ariel Corner, 3030 Limassol, Cyprus., or electronically at dpo@priorcapital.eu

Complaints may also be lodged to the supervisory authority in Cyprus (Office of the Commissioner for Personal Data Protection, by post at 1 Iasonos Str. 1082, Nicosia, Republic of Cyprus. More information can be found at http://www.dataprotection.gov.cy.