



# PRIVACY POLICY

HuaPrime EU Ltd  
License Number: 426/23  
Date: 31 July 2024  
Version: 2

The Privacy Notice is meant for use by HuaPrime EU Ltd (ex Ultima Markets Cyprus Ltd - hereinafter “the Company” and/or “us” and/or “we”), and its Employees.

HuaPrime EU Ltd (ex Ultima Markets Cyprus Ltd) is authorized by the Cyprus and Securities and Exchange Commission (CySEC) under license number 426/23 to provide Investment and Ancillary services, and is obliged to strictly observe relevant laws, directives, and applicable legislations. The company is compliant with the requirements of the Markets in Financial Instruments Directive II (MiFID II) and Regulation (EU) No 600/2014 of the European Parliament and the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (the “MiFIR”), Investments Services Law 87(I) 2017-2023, the laws for the Prevention of Money Laundering and Terrorist Financing, Market Abuse and Insider Dealing, the General Data Processing Regulation as well as other legislations applicable in the Republic of Cyprus.

The Company has established this Privacy Notice in accordance with General Data Processing Regulation (GDPR) and laws, regulations and/or directives issued pursuant to this Law.

This Privacy Notice applies to former, existing and potential Employees of the Company.

“Employee” means any natural or legal person who works part-time or full-time under the contract of employment signed between the Employee and the Company and has recognized rights and duties and being paid on a monthly basis.

This Privacy Notice aims to provide our Employees with information on what type of information we collect, how it is used and the circumstances where such information could be shared with third parties.

### **The present Privacy Notice:**

- provides an overview of how the Company collects, processes and uses your personal data and informs you about your rights under the local data protection law and the EU General Data Protection Regulation (“GDPR”);
- contains information about when we share your personal data with other third parties (for example the Office of the Commissioner for Personal Data Protection located in Cyprus, or within the Group where the Company belongs).

We endeavor to ensure that sensitive personal data is only shared with colleagues with your explicit consent.

Through this privacy notice, your data may be called either “personal data” or “personal information”. We may also, sometimes, collectively refer to handling, collecting, protecting and storing your personal data or any such action as “processing”.

For the purposes of this notice, personal data shall mean any information relating to you which identifies or may identify you, including, for example, your name, address and identification number.

The present Privacy Notice aims to help you better understand the most recent changes to the Privacy Policy and how they may impact you.

## Collection of Personal Data:

The Company shall collect information necessary to fulfil their legal and regulatory obligations as well as for the purposes of overseeing and monitoring who enters the Company's premises and has access to sensitive and confidential information.

We will gather information and documentation to personally identify, contact or locate you and may gather information from third parties and/or other sources in order to achieve the same. As a customer of the Company, you are responsible for the true and accurate information and to keep us informed of any changes to your personal information or circumstance by emailing us at [dpo@huaprime.eu](mailto:dpo@huaprime.eu).

## How your personal data is used by the Company

Your data is used by us for a number of purposes including:

- Internal reporting and record keeping
- Responding to data access requests you make
- Giving key card access to the office
- Contacting you, or other relevant contact in case of an emergency
- Providing staff accommodation

## Sharing your data with others

Within the Company, personal data, including sensitive personal data, may be shared between members of staff, who legitimately need the information to carry out their duties (i.e., Company's Compliance Officer or Data Protection Officer). We endeavor to ensure that sensitive personal data is only shared with colleagues with your explicit consent.

However, circumstances may arise where this data is shared with colleagues without gaining your consent. This will only occur if it is necessary to protect your vital interests or the vital interests of another person; or for certain other reasons where it is not possible or appropriate to gain your consent such as disclosures to the police for prevention or detection of crime.

The Company may disclose certain personal data to third parties. These external organizations, and the purpose for sharing the information, are set out below:

1. Within the Group where the Company belongs.
2. Internal and External Auditors of the Company for reporting purposes if necessary
3. IT providers for technical and/or other similar purposes

Otherwise, the Company does not share data with any third party, except as required by law. We do not sell your personal data to third parties under any circumstances or permit third parties to sell on the data we have shared with them.

## Transfer of personal data to other countries

Where data is shared within the European Union (EU) or other third countries, the third party will be required to comply with and safeguard the data under the terms of the DPA and appropriate EU regulations.

## **Who Controls and Processes Your Personal Data**

The relevant departments of the Company, such as Compliance, Human Resources (HR), Accounting and Finance and Back Office, as well as any undertakings being a member of our group, agents which we engage with for the purpose of collecting, storing and processing personal data and any third parties acting on our or their behalf, may collect, process and store personal data provided by you.

For the purpose of processing and the storage of personal data provided by you in any jurisdiction within the European Union or outside of the European Union, the Company can confirm this will be done in accordance with applicable laws.

## **Period of Keeping Your Personal Information**

The Company will keep your personal data for as long as an employment relationship exists within the Company. Once the employment relationship with you has ended, we are required to keep your data for a maximum period of five (5) years to meet our regulatory and legal requirements.

If reasonably necessary or required to meet other legal, contractual or regulatory requirements, resolve disputes, prevent fraud and abuse, or enforce our terms and conditions, we may also keep some of your information for three (3) years in addition as required, even after the previously mentioned period. When we no longer need such personal data, we securely delete or destroy it.

## **Your Rights**

### **Your Rights to Access**

You have the right to request copies of your personal data.

Information must be provided, without delay and at the latest, within one month of request. The Company will be able to extend the period of compliance by an additional two (2) months when requests are complex or numerous. If that is the case, we will inform the Employee within one (1) month of the receipt of the request and explain why the extension is necessary.

### **Can the Company charge a fee for dealing with a subject access request?**

You have the right to be provided with a copy of the personal data undergoing processing, free of charge. For any further copies requested, the Company may charge a reasonable fee based on administrative costs.

### **When should personal data be rectified?**

The GDPR includes a right for Employees to have inaccurate personal data rectified or completed if it is incomplete.

You can make a request for rectification either verbally or in writing.

If we have disclosed the personal data in question to others, we shall contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort. If asked to, we shall also inform the individuals about these recipients.

### **How long does the Company have to comply with a request for rectification?**

We shall respond within one month.

This can be extended by two (2) months if the request for rectification is complex.

In cases where the Company is not taking action in response to a request for rectification, we must explain the why to the Employees, informing them of their right to complain to the supervisory authority and to a judicial remedy.

## **Your Right to Erasure;**

### **When does the right to erasure apply?**

The right to erasure does not provide an absolute ‘right to be forgotten’. Employees have a right to have personal data erased and to prevent processing in specific circumstances.

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the Employee withdraws consent.
- When the Employee objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

There are some specific circumstances where the right to erasure does not apply and we can refuse to deal with such a request.

We have a legal obligation to obtain data on you while meeting relevant regulatory obligations; based on the legal obligations imposed on us, Employees shall have no right to erasure, no right to data portability or right to object on the information gathered meeting with our legal obligation under our license to provide financial services.

### **When can the Company refuse to comply with a request for erasure?**

We can refuse to comply with a request for erasure when the personal data is processed for the following reasons:

- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- the exercise or defense of legal claims.

Does the Company have to tell other organizations about the erasure of personal data?

If we have disclosed the personal data in question to others, we must contact each recipient and inform them of the erasure of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, we must also inform the Employees about these recipients.

## **Your Right to Restrict Processing:**

### **When does the right to restrict processing apply?**

We will be required to restrict the processing of personal data in the following circumstances:

- When an Employee contests the accuracy of the personal data, we should restrict the processing until you have verified the accuracy of the personal data.
- When an Employee has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests) and we are considering whether our Company organization's legitimate grounds override those of the Employee.
- When processing is unlawful, and the Employee opposes erasure and requests restriction instead.
- If the Company no longer needs the personal data, but the Employee requires the data to establish, exercise or defend a legal claim.

We may need to review procedures to ensure we are able to determine when we may be required to restrict the processing of personal data.

If the Company has disclosed the personal data in question to others, we must contact each recipient and inform them of the restriction on the processing of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, we must also inform the Employees about these recipients.

The Company must inform Employees when we decide to lift a restriction on processing.

### **Your Right to Data Portability**

- The right to data portability allows Employees to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- We shall respond to such a request without undue delay and within one (1) month. This can be extended by two (2) months if the request is complex or when the company may receive a number of requests. We will inform the individual within one (1) month of the receipt of request and explain why the extension is necessary, if applicable.

### **Your Right to Object**

Employees have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling);
- processing for purposes of scientific/historical research and statistics.

We will stop processing the personal data unless:

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defense of legal claims.

### **Geographical Area of Processing:**

As a general rule, the Employee data is processed within the European Union/European Economic Area (EU/EEA), but in some cases it is transferred to and processed in countries outside the EU/EEA. The transfer and processing of Employee data outside the EU/EEA can take place, provided there are appropriate safeguards in place and the actions are made on a legal basis only. Upon request, the Employee may receive further details on Employee data transfers to countries outside the EU/EEA.

### **Other Related Information**

We use appropriate technical, organizational and administrative security measures to protect any information we hold in our records from loss, misuse, and unauthorized access, disclosure, alteration and destruction. Unfortunately, no company or service can guarantee complete security. Unauthorized entry or use, hardware or software failure, and other factors may compromise the security of user information at any time.

Transmission of information via regular email exchange is not always completely secure. The Company, however, exercises all possible actions to protect Employees' personal data, yet it cannot guarantee the security of Employee data that is transmitted via email; any transmission is at the Employee's own risk. Once the Company has received the Employee information it will use procedures and security features in an attempt to prevent unauthorized access.

### **Raising a Concern**

You have the right to be confident that we handle your personal information responsibly and in line with good practice.

If you have a concern about the way we are handling your information, for example, if you feel we may not be;

- keeping your information secure;
- holding accurate information about you;
- disclosing information about you
- deleting or archiving information about you beyond the necessary period of time; or
- collecting information for legitimate reasons, in accordance to laws and regulations;

We take all concerns seriously and will work with you to resolve any such concerns. Any concerns and/or requests can be raised to the appointed Data Protection Officer, whose contact details are below:

#### **HuaPrime EU Ltd (ex Ultima Markets Cyprus Ltd)**

**Georgiou Griva Digeni 122A,  
Kallinicos Court, shop 1 - Upper level,  
Neapolis, 3101 Limassol, Cyprus**

**Tel: +357 25747775**

**Email: [contactus@huaprime.eu](mailto:contactus@huaprime.eu) or [dpo@huaprime.eu](mailto:dpo@huaprime.eu)**

If you are not satisfied with any responses provided by us, you have the right to raise such matters with the Cyprus Data Protection Commissioner. Contact details are below:

#### **Office of the Commissioner for Personal Data Protection**

1 Iasonos str.,  
1082 Nicosia P.O.Box 23378,  
Tel: +357 22818456  
Fax: +357 22304565  
Email: [commissioner@dataprotection.gov.cy](mailto:commissioner@dataprotection.gov.cy)

The Employee has the right go to court or to escalate their complaint to the data protection regulator in their jurisdiction for the protection of rights, unless the applicable laws prescribe a different procedure for handling such claims.

### **Changes to this Privacy Notice**

The Company reserves the right to modify or amend this Privacy Notice unilaterally, at any time, in accordance with this provision.

If any changes are made to this privacy notice, we shall notify you accordingly.

The revision date shown at the beginning of this Privacy Notice will also be amended. We do, however, encourage you to review this privacy notice occasionally in order to stay informed about how we are processing and protecting your personal information.

### **Monitoring and Review**

The Company will monitor, on a regular basis, the effectiveness of this Privacy Notice and, in particular, the execution quality of the procedures explained in the Privacy Notice; where appropriate, the Company reserves the right to correct any deficiencies.

In addition, the Company will review the Privacy Notice at least annually.

The Company will inform its Employees of any material change to this Privacy Notice by emailing an updated version of this Privacy Notice.

### **Definitions**

“**Personal Data**” means any information relating to an identified or identifiable natural person (‘data subject’); 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

“**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;

“**Processor**” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

“**Consent**” of the employee means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

“**Profiling**” means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

HuaPrime EU Ltd (ex Ultima Markets Cyprus Ltd) is regulated by CySEC with the license number 426/23 · <https://huaprime.eu/>