The Ultima World (DIFC) Limited respects your privacy and is committed to protecting your personal data. This privacy notice will inform you as to how we look after your personal data and tell you about your privacy rights and how the law protects you.

You are receiving a copy of this privacy notice because you are applying for work with us (whether as an employee, worker or contractor). It makes you aware of how and why your personal data will be used, namely for the purposes of the recruitment exercise, and how long it will usually be retained for, in accordance with the General Data Protection Regulation.

It is important that you read this privacy notice together with any other privacy notice or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data.

1. IMPORTANT INFORMATION AND WHO WE ARE

We are a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

Data Protection Officer

We have appointed a data protection officer ("DPO") who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the DPO using the details set out below.

Contact details

Full name of legal entity: The Ultima World (DIFC) Limited (also trading as The Ultima World. Wealth Management Platform)

Name of DPO: Ms. Mariia Georgievskaia

Email address: dpo@theultima.com

Postal address: Unit 1002, Level 10, Index Tower, Dubai International Financial Centre, Dubai, P. O. Box 507341, United Arab Emirates

Website: theultima.com

You have the right to make a complaint at any time to the Information Commissioner's Office, the DIFC supervisory authority for data protection issues using the following contact details:

Dubai International Financial Centre Authority

Postal address: Level 14, The Gate Building

Phone number: +971 4 362 2222

Email address: commissioner@dp.difc.ae

We would, however, appreciate the chance to deal with your concerns before you approach the Commissioner's Office so please contact us in the first instance.

2. DATA PROTECTION PRINCIPLES

We comply with the requirements of the Data Protection Law 2020 of Dubai International Financial Centre ("**Law**") and any associated legal documents. According to the Law, the principles relating to processing of personal data should be followed. In light of this, the personal data received from you and held with us must be:

- Processed on a lawful basis;
- Processed lawfully, fairly and in a transparent way;
- Processed only for specified, explicit and legitimate purposes and not in any way that is incompatible with those purposes;
- relevant to the purposes we have told you about and limited only to what is necessary for those purposes;
- Accurate and kept up to date;
- Kept only as long as necessary for the purposes we have told you about;
- Kept securely.

3. THE DATA WE COLLECT ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "**special categories**" of more sensitive personal data, which require a higher level of protection and specific justification to process them.

We may collect, use, store and transfer different kinds of personal data about you, which we have grouped together as follows:

- Identity Data: first name, maiden name, last name, title, date of birth, place of birth, nationality, gender, passport or ID details, driving license details, national insurance number, medical insurance number, photographs.
- Family Data: marital status, information about family members and co-habitants.
- Contact Data: residence address, mailing address, email address, telephone numbers, fax number, next of kin and emergency contact information.
- Education Data: level of education, major strands, details of school, college and university diplomas, professional qualifications, trainings, workshops and seminars, computer skills.
- Employment Data: recruitment information (references and other information included in a CV or cover letter or as part of the application process), work history, including start and termination

dates, employers' names, location of employment, job title, responsibilities, disciplinary and grievance information, disqualifications records, details of any license, authorisation, registration, notification, membership or other permission granted or revoked by any governmental or statutory authority or any other regulatory or self-regulatory body, any censure, discipline, suspension, fines or investigation by any regulatory or self-regulatory body.

- Financial Data: bank account details, tax status information, tax identification number, securities and shareholdings, bankruptcy records.
- Special categories of personal data: criminal convictions: details of criminal convictions and offences of fraud, theft, false accounting, serious tax offences (including without limitation tax evasion or the facilitation of tax evasion offences), market manipulations or insider dealing; information about medical condition.

We also collect, use and share aggregated anonymized data such as statistical or demographic data for any purpose. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does **not** directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature.

However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data, which will be used in accordance with this privacy notice. We will ask your separate consent for these purposes.

If you fail to provide personal data

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully. For example, if we require references for this role and you fail to provide us with relevant details, we will not be able to take your application further.

4. HOW IS YOUR PERSONAL DATA COLLECTED?

We collect personal information about you through the application and recruitment process from the following sources:

- You, the candidate.
- Recruitment agencies.
- Background check providers.
- Disclosure and Barring Service in respect of criminal convictions.
- Your named referees.
- Publicly accessible sources.

5. HOW WE USE YOUR PERSONAL DATA

We will use the personal information we collect about you to:

- Assess your skills, qualifications, and suitability for role.
- Carry out background and reference checks, where applicable.
- Communicate with you about the recruitment process.
- Keep records related to our hiring processes.
- Perform equal opportunities monitoring.
- Comply with legal or regulatory requirements.
- Establish, defend or remedy claims, including discrimination claims or other legal actions involving job applicants.

It is in our legitimate interests to decide whether to appoint you to role since it would be beneficial to our business to appoint someone to that role.

We also need to process your personal information to decide whether to enter into a contract of employment with you.

Having received your CV, covering letter and your application form, we will then process that information to decide whether you meet the basic requirements to be shortlisted for the role. If you do, we will decide whether your application is strong enough to invite you for an interview. If we decide to call you for an interview, we will use the information you provide to us at the interview to decide whether to offer you the role. If we decide to offer you the role, we will then take up references and carry out a criminal record and bankruptcy record check before confirming your appointment.

How we use particularly sensitive personal information

We will use your particularly sensitive personal information to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments with respect to your disability status need to be made during an interview.

Information about criminal convictions

We envisage that we will process information about criminal convictions.

We will collect information about your criminal convictions history if we would like to offer you the role conditional on checks and any other conditions, such as references, being satisfactory. We are entitled to carry out a criminal records check in order to satisfy ourselves that there is nothing in your criminal convictions history, which makes you unsuitable for the role. We have in place an appropriate policy document and safeguards, which we are required by law to maintain when processing such data.

Consent

Generally, we do not rely on consent as a legal basis for processing your personal data. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly

sensitive data or criminal convictions records. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis, which allows us to do so.

Automated decision-making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making.

7. DATA SECURITY

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

Specifically, we implement the following technical and organizational security measures to protect your personal data:

- Pseudonymisation of personal data.
- Encryption of personal data.
- Segregation of personal data from other networks.
- Access control and user authentication.
- Employee training on information security.
- Written information security policies and procedures.

In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and are subject to a duty of confidentiality.

We have also put in place procedures to deal with any suspected data security breach and will notify you and the Comissioner's Office of a suspected breach where we are legally required to do so. Further details of these measures may be obtained from our DPO.

8. DISCLOSURES OF YOUR PERSONAL DATA

We may share your personal data with the parties listed below for the purposes set out in section 4 above:

- Our staff members.
- Parent company, subsidiaries, and affiliated entities.

- Governmental, regulatory or similar authorities or industry bodies.
- Courts or tribunals of competent jurisdiction.
- Law enforcement officials.
- Third-party service providers, such as background check providers.

International transfers

We may share your personal data with external third parties based outside the DIFC.

Whenever we transfer your personal data outside the DIFC, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We transfer your personal data to jurisdictions that have been deemed to provide an adequate level of protection for personal data by the Commissioner of Data Protection. For further details, see DIFC: Adequate Data Protection Regimes, here https://www.difc.ae/business/registrars-and-commissioners/commissioner-of-data-protection/data-export-and-sharing
- We have entered into specific contracts approved by the Commissioner, which give personal data the same protection it has in the DIFC. For further details, see DIFC: Data Protection Forms/Standard Data Protection Clauses approved for use in accordance with Article 27(2)(c) regarding transfers of Personal Data outside of the DIFC in the absence of an adequate level of protection, here https://www.difc.ae/business/registrars-and-commissioners/commissioner-of-data-protection/data-export-and-sharing
- The transfer is necessary to enter into or perform our contract with you or in your interest or to establish, exercise or defend legal claims, or we are required to do so under foreign laws applicable to us, or subject to international financial standards, the transfer is necessary to uphold our legitimate interests recognized in international financial markets, in relation to the latter except were our interests overridden by your legitimate interests relating to your particular situation.

Suitable additional safeguard we may provide for international transfers includes:

- a transfer of pseudonymized or encrypted data;
- ensuring with technical and organizational measures that the transferred data cannot be used for other purposes than those strictly foreseen by us;
- limiting the purposes for which the data may be processed following the transfer;
- ensuring deletion of the data as soon as possible after the transfer;
- obliging data recipients to implement adequate technical and organizational security measures, inform us about binding requests for disclosure and any accidental or unauthorised access, respond to our enquiries, request our approval in the event of sub-processing.
- recording all relevant aspects of data transfer.

9. HOW LONG WILL WE USE YOUR PERSONAL DATA?

Subject to any exceptional circumstances or to comply with laws or regulations that require a specific retention period, we will retain personal information about you for a period of 6 months after we have communicated to you our decision about whether to appoint you to the role or position applied for. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal information.

10. YOUR LEGAL RIGHTS

Under certain circumstances, you have rights under data protection laws in relation to your personal data.

If you wish to exercise any of the rights set out below, please, contact our DPO.

You have the right to:

Request access to your personal data (commonly known as a "**data subject access request**"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request rectification of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons, which will be notified to you, if applicable, at the time of your request.

Object to processing of your personal data 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 legitimate interests.

You also have the right to object where we are processing your personal data for direct marketing and analytical purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information, which override your rights and freedoms.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

- if you want us to establish the data's accuracy;
- where our use of the data is unlawful but you do not want us to erase it;

- where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
- you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

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.

Withdraw consent at any time 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 your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one 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.

11. CHANGES TO THE PRIVACY NOTICE AND YOUR DUTY TO INFORM US OF CHANGES

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

This version was last updated on 5 December 2024 and historic versions are archived on our website theultima.com or can be obtained by contacting our DPO.