ANDURANDCAPITAL

EMPLOYEES AND CANDIDATES' PRIVACY NOTICE

Your privacy is very important to us. This notice ("**Privacy Notice**") is provided by Andurand Capital Management Ltd (the "Manager"), Andurand Capital Management LLP (the "Investment Manager, Andurand Capital Management (DIFC) Limited (the "Sub- Investment Manager" or "ACMDL")and Andurand Ventures Limited ("AVL") (collectively "**we**" or "**us**") and sets out our policies with respect to the collection, sharing and use of personal information.

ACMDL is registered under the laws of the Dubai International Financial Centre ("DIFC") and is a "Controller" of your Personal Data, meaning we are responsible for Processing your Personal Data. We are committed to protecting your privacy and Processing your Personal Data fairly and lawfully in compliance with the DIFC Data Protection Law No.5 of 2020 ("DIFC DPL").

This notice applies to all candidates and employees, including contractors, temporary workers, directors and secondees of whom we process their Personal Data and are employed by us or are considering employment with us. Any reference to "Data Subject", "you" or "your" in this privacy notice refers to the applicable list above, as the context requires unless otherwise stated.

This Notice does not form part of your contract of employment or engagement and may be amended from time to time in line with best practice and any changes in the law or applicable codes of practice.

How we collect information about you

We may collect personal data about you through:

- information provided directly to us by you, or another person on your behalf, by email or post, or in person;
- recording and monitoring of telephone conversations and electronic communications with you as described below; or
- the use of Internet "cookies" (an information collecting device from a web server), as described further below.

We may also, in some circumstances, receive personal information about you from third parties, such as previous employers, recruitment agencies, regulatory or law enforcement agencies, agencies conducting background check provider. Personal information may also be obtained from publicly accessible sources of information, such as public databases, industry associations, social media and online professional networks.

For ACMDL employees- the DIFC DPL requires companies to have a "legal basis" to Process Personal Data. Most commonly, this will be:

- to comply with our legal and regulatory obligations;
- for the performance of our contract with you or to take steps at your request before entering into a contract;
- in limited circumstances, where you have given consent;
- for vital interests (e.g. emergency situation); or
- where it is necessary for legitimate interests pursued by us or a third party and your interests and fundamental rights do not override those interests e.g. for security purposes or to transfer Personal Data without our group for HR or admin purposes.

In cases of Special Category Personal Data, we will also need to have further justification for Processing this, such as:

- in limited circumstances, we have your explicit written consent;
- it is necessary for the purposes of carrying out the obligations of being your employer and to exercise our rights as your employer;
- vital interests;
- it is necessary for the establishment, exercise or defence of legal claims; and
- it is necessary for the purposes of complying with regulatory requirements relating to unlawful acts and dishonesty, malpractice or other seriously improper conduct.

ACMDL will process your Personal Data for the following purposes and with reliance on the listed legal bases:

Processing Purpose	**Legal Basis**
For the administration of your employment including: • determining the terms on which you work for us • To check you are legally entitled to work in the UAE • making decisions about salaries and promotions • administering payroll and handling pension payments such as DEWS[1] • providing and administering employee benefits and pensions • providing training and development opportunities • conducting performance management and sickness and absence management • recording emergency contacts • undertaking grievance and disciplinary procedures • conducting business continuity planning • planning corporate event and activities • making decisions about your continued employment or engagement or making arrangements for the termination of our working relationship	• To enter into a contract / Performance of contract/ As necessary to exercise our rights and carry out our obligations as your employer • Legitimate interests (Employee Management, Training and Welfare) • To comply with our legal obligations under employment law • We have your consent (e.g. in relation to providing/making available certain employee benefits to you)
• For internal finance management, including personnel expense reimbursement, travel and time-keeping	• Legitimate interests (Business Administration and Operations) • Performance of contract • To comply with our legal obligations (for example recording compliance

[1] The DIFC Employee Workspace Savings Plan

	with national minimum wage or working time)
• For monitoring and assessing compliance with our policies and standards	• Legitimate interests (Employee Management, Training and Welfare) • Performance of contract • To comply with our legal obligations (for example recording compliance with staff training requirements)
• To consider your suitability for any of our current or future employment opportunities and to confirm your references, character and educational background and conducting background checks	• To enter into a contract / Performance of contract • Legitimate interests (Employee Management)
• To comply with our legal and regulatory obligations (both local and international) (e.g. employment law)	• To comply with our legal and regulatory obligations
• To comply with court orders or requests from regulatory bodies or law enforcement regulatory agencies and other public and government authorities, which may include such authorities outside your country of residence	• To comply with our legal and regulatory obligations
• General business management, operations and planning, including accounting and auditing	• Performance of contract • To comply with our legal and regulatory obligations • Legitimate interests (Business Administration and Operations)
• For administrative purposes in ensuring the security and access of our systems, premises, platforms and secured websites and applications	• Legitimate interests (Business Administration and Operations)
• To record health and safety incidents	• To comply with our legal obligations • As necessary to exercise our rights and carry out our obligations as your employer
• In the pursuance, establishment or defence of legal claims arising out of or in connection with your employment/engagement with the business	• As necessary to exercise our rights and carry out our obligations as your employer • Legitimate interests (Business Administration and Operations)
• Investigation or fraud prevention	• Legitimate interests (to detect and prevent fraud and carry out any necessary investigations)

• In connection with a business Transaction (as defined below) such as merger, restructuring or sale of the business or business strategies	• Legitimate interests (Business Administration and Operations) • To comply with our legal obligations
• To monitor your use of our information and communication systems to ensure compliance with our IT policies and to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution	• Legitimate interests (Business Administration and Operations) • As necessary to exercise our rights and carry out our obligations as your employer
• To contact your next of kin, for instance, in order to meet the employees welfare needs in the event of an incident/accident	• Legitimate interests (Employee Management, Training and Welfare) • As necessary to exercise our rights and carry out our obligations as your employer

Some of the above lawful bases for processing will overlap and there may be several lawful bases which justify our use of your Personal Data.

Why we collect information about you

We are required to keep and Process your Personal Data for employment purposes. The information that we hold, and Process will be used for management and administrative use only. We will keep and use your personal data to enable us to carry out our business and management of the employment relationship with you effectively, lawfully, and appropriately, during the recruitment stage, whilst you are employed by us and at the time your employment ends. This includes information that enables us to comply with the employment contract, any legal requirements, and for us to protect our legal position in the event of any legal proceedings.

If you do not provide this data, we may in some circumstances be unable to comply with our legal and regulatory obligations. Under such circumstances, we will inform you of the implications of that decision.

We will use one of the permitted grounds under the applicable law to process your information. Such grounds include instances where you have given your consent and cases where your consent is not required under applicable law, such as where we are required to comply with a legal obligation such as performance of a contract or to comply with an appliable law, or where we or a third party determine that is necessary for our legitimate interests to collect and use your personal information (except where this is overridden by the rights of the data subject, or where processing is necessary to protect vital interests. Employees family members / dependants are also covered under this notice to the extent they form part of the benefits under the employment contract

In the case of processing data related to your Covid-19 Health Records (as defined on the next page), we will also use one of the permitted grounds under the applicable law to process such information. We will only use this information to help with our office layout planning and to coordinate a schedule of who will be working from the office, to safeguard all employees' best interests. We will not use this information to discriminate, in any shape or form, against any employee.

The legitimate interests to collect your personal information may include any of the purposes identified above and any other purpose where we or a third party have determined that you have a reasonable expectation for us or a third party to collect or use your personal information for such purpose.

What are the consequences of failing to provide your personal information?

As a regulated financial services firm, we are subject to legal and regulatory obligations that may require us to collect and store your personal information, such as the requirements to comply with the applicable law on prevention of financial crime, tax and regulatory reporting, or the rules on recording and monitoring of communications (as described below).

We may also need to collect and use your personal information for the purposes of entering into or performance of a contractual arrangement between us.

A refusal to provide us with personal information may, depending on the purpose for which your personal information is required, have various consequences such as us being unable to communicate with you, the termination of a contractual arrangement between us, or, where we have a reasonable suspicion of illegal activity, we may be required to make a report to regulatory or enforcement agencies.

The types of personal data we may collect and use

Under GDPR, the categories of personal data we may collect will depend on the nature of our relationship with you and the purpose of which information is being collected. Such personal data may include names, residential and work addresses or other contact details such as phone number, signature, nationality, date and place of birth, national insurance or other tax identification number, photographs, copies of identification documents, bank account details, , criminal and administrative offences, , as well as special categories of data, information about a person's ethnic origin, health, or other sensitive information. As at the time of writing, the only special category data we process relates to: [i] your vaccination status in relation to Covid-19, and [ii] when requested by the Chief Operations Officer, an update on your recent health status and the results with respect to tests in relation to the Covid-19 virus; collectively referred to as "Covid-19 Health Records".

ACMDL typically process the following additional types of personal data about you:

- personal details such as gender, marital status, emergency contact details, country of residence, next of kin and emergency contact information;
- professional details such as your CV, details of your qualifications, location of employment and workplace, employment history, certifications, biography, relevant experience and skills;
- financial information such as salary, payroll records, tax related details, DEWS, pension and benefits information;
- recruitment information, including copies of right-to-work documentation, information required for the provision of medical insurance, employment references and other information included as part of the application process;
- response to internal surveys and other internal communications;
- identification documentation such as copies of your passport, driving licence, national ID card, employment visa, or other documentation required by law (which may include your photograph);
- HR-related records such as training, appraisals/performance assessments, annual leave, absence and time-keeping records, disciplinary, grievance or capability proceedings, references and background checks; and
- details of your access to our premises and systems, software, websites, and applications including access, location data and communications data.

Certain categories of personal data require special protection under the law and this is known as "special category data". We typically process the following types of special category data:

- information about your health, including any medical conditions and health and sickness records;

- information about your criminal convictions and offences collected from background checks conducted at the beginning of your employment or engagement with us; and

visa application details such as religion.

We make every effort to maintain the accuracy and completeness of your Personal Data which we store and to ensure all your Personal Data is up to date. However, you can assist us with this considerably by promptly contacting us if there are any changes to your Personal Data or if you become aware that we have inaccurate Personal Data relating to you.

Do we share your personal information with third parties?

We may (to the extent relevant to the purpose for which we collect your information), share your personal data with third parties, such as:

- our affiliates or other entities that are part of our group or with our clients;
- any person to whom we have a right or obligation to disclose personal data, or where we determine that disclosure is necessary to protect or defend our rights or property, including with regulators, courts of law, governmental, regulatory or law enforcement agencies and any other public authorities which may include such authorities outside your country of residence;
- our internet, IT, telecommunications and other service providers, including legal advisers, accountants, payroll administrators, insurance and employee benefits providers and administrators;
- service providers and trading counterparties to our clients, including placement agents or distributors, brokers, banks, trading venues, clearing houses, custodians, corporate services providers, administrators of our funds, and providers of customer relationship management tools;
- other third parties conducting background checks in the context of employment
- any person, as directed by you; or
- any person to whom we transfer any of our rights or obligations under any agreement, or in connection with a sale, merger or consolidation of our business or other transfer of our assets, whether voluntarily or by operation of law, or who is otherwise deemed to be our successor or transferee.
- when required to third parties to protect our rights, users, systems and services.

Transfers of Personal Data

Due to the international nature of our business, your personal data may be transferred to countries outside of the European Economic Area ("EEA") or the DIFC, such as to jurisdictions where we or have a service provider, including countries that may not have the same level of data protection as that afforded by the EU General Data Protection Regulation or the DIFC DPL and other data protection rules applicable to us (collectively, "**Data Protection Law**"). In these circumstances, we take steps to ensure that the recipient agrees to keep your information confidential and that it is held securely in accordance with the requirements of Data Protection Law, such as by requesting appropriate contractual undertakings, such as data processing agreements or standard contractual clause in our legal agreements with service providers and group entities or relying on one of the appropriate derogations set out in Data Protection Law. You may ask us for further details of these safeguards, where required.

For how long do we keep your personal information?

We will generally keep personal information about you for as long as necessary in relation to the purpose for which it was collected, or for such longer period if required under applicable law or necessary for the purposes of our other legitimate interests.

The applicable retention period will depend on various factors, such as any legal obligation to which we or our service providers are subject as well as on whether you decide to exercise your right to request the deletion of your information from our systems. As a minimum, information about you will be retained for the entire duration of any business employment relationship we may have with you, and for a minimum period of five to seven years after the termination of any such relationship.

In the DIFC, in general, Personal Data relating to employment is retained for a period of 6 years from the date of termination. We will retain the Personal Data of unsuccessful candidates for a period of 1 year following the date of rejection.

We will, from time to time, review the purpose for which we have collected information about you and decide whether to retain it, update it, or securely delete it, if the information is no longer required.

What are your rights?

You have certain rights under Data Protection Law in respect of the personal data we hold about you and which you may exercise. These rights are:

- to request access to your information;
- to request rectification of inaccurate or incomplete information;
- to request erasure of your information (a "right to be forgotten");
- to restrict the processing of your information in certain circumstances;
- to object to processing where personal data is being processed for direct marketing purposes and a legitimate interests;
- where relevant, to request the portability of your information;
- where you have given consent to the processing of your data, to withdraw your consent; and
- to lodge a complaint with the competent supervisory authority.
- In the DIFC, you have the right not to be discriminated against for exercising your rights.

You should note that your right to be forgotten that applies in certain circumstances under Data Protection Law is not likely to be available in respect of the personal data we hold, given the purpose for which we collect such data, as described above.

How to contact us

If you have any questions about this Privacy Notice or requests with regards to the personal data we hold about you, please contact the Chief Compliance Officer at compliance@andurandcapital.com or by writing to the Manager at The Hedge Business Centre, Level 5, Ir-Rampa ta' San Giljan, Balluta Bay, St Julian's, STJ1062 or the Investment Manager or AVL at 100 Brompton Road, London SW3 1ER, United Kingdom or ACMDL at: Level 1, DIFC Fund Centre, Precinct Building 4, Dubai International Financial Centre, Dubai, United Arab Emirates.

Complaining to Relevant Authorities

You have the right to complain to the Office of the Information and Data Protection Commissioner (IDPC) in Malta with regards to the Manager or the Information Commissioner's Office (ICO) if the complaint relates to the Investment Manager. Further information is available from the IDPC's website or the ICO's website.

In the DIFC, if you are not satisfied with our response or believe we are not processing your personal data in accordance with the law, you can escalate your complaint to the data protection supervisory authority via the details below:

DIFC Data Protection Commissioner
Contact Details:
Dubai International Financial Centre Authority Level 14,
The Gate Building
+971 4 362 2222
commissioner@dp.difc.ae

Recording and monitoring of communications

We may record and monitor telephone conversations and electronic communications with you for the purposes of:

- ascertaining the details of instructions given, the terms on which any transaction was executed or any other relevant circumstances;
- ensuring compliance with our regulatory obligations; or
- detecting and preventing the commission of financial crime.

Copies of recordings will be stored for a period of five years, or such other longer period as we may determine from time to time.

How we update or change this Notice

We may change or update parts of this Notice in order to maintain our compliance with the Appliable Data Protection Law's or following an update to our internal practices. Therefore, please ensure that you regularly check this Notice so you are fully aware of any changes or updates. We will inform you of any material changes to this Notice.

This Notice was last updated in September 2025.