

Data Protection Privacy Notice (Recruitment) (“Notice”)

Old Mission Europe LLP (“**Old Mission Europe**”) is a limited liability partnership incorporated under the laws of England and Wales, registered under number OC403724, and having its registered office address at 1 Finsbury Square, 4th Floor, London, England, EC2A 1AE.

Old Mission Europe is registered as a data controller with the UK Information Commissioner’s Office under registration number ZB065392 and is authorised and regulated by the Financial Conduct Authority (“**FCA**”).

Old Mission Europe is a ‘controller’ of personal data and gathers and uses certain data about you. This data is also used by Old Mission Europe’s affiliated entities and group companies, namely Old Mission Capital LLC (“**Old Mission Capital**”). References in this Notice to the “**Company**”, “**we**”, “**our**”, or “**us**” are references to Old Mission Europe and its affiliated entities as applicable.

This Notice reflects our commitment to safeguarding the privacy and security of our candidate data and explains what personal data (information) we hold about you, how we collect it, and how we use and may share data about you during the recruitment process. Please ensure that you read this Notice and any other similar notice we may provide to you from time to time when we collect or process personal data about you.

This Notice does not form part of any contract of employment or other contract to provide services. We may update this Notice at any time but if we do so, we will provide you with an updated copy of this Notice as soon as reasonably practical.

Data protection principles

The Company will comply with the following data protection principles when processing personal data:

- we will process personal data lawfully, fairly, and in a transparent manner (“**lawfulness, fairness, and transparency**”);
- we will collect personal data for specified, explicit, and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes (“**purpose limitation**”);
- we will only process the personal data that is adequate, relevant, and necessary for the relevant purposes (“**data minimisation**”);
- we will keep accurate and up to date personal data and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay (“**accuracy**”);
- we will keep personal data for no longer than is necessary for the purposes for which the data are processed (“**storage limitation**”);

- we will take appropriate technical and organisational measures to ensure that personal data are kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage (“**security, integrity, and confidentiality**”);
- we will not transfer personal data to another country without appropriate safeguards in place (“**transfer limitation**”); and
- we will make available to data subjects and allow data subjects to exercise certain rights in relation to their personal data (“**data subject’s rights and requests**”).

We are also responsible for, and must be able to demonstrate compliance with, the data protection principles set out above (“**accountability**”).

About the data we may collect and hold

We will hold “**personal data**”, or “**personal information**”, which refers to any information about an individual from which that person can be identified. It does not include data where the person’s identity has been removed (anonymous data).

The table below summarises the data we collect and hold, how and why we do so and how we use it.

Special categories of personal information

Some of the personal information which you provide to us, or which we may receive, may constitute “special categories” of personal information. This is personal information revealing a person’s racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, genetic data, biometric data, sex life, sexual orientation, or data concerning health. We process special categories of personal information on the basis of one or more of the following:

- where you have given explicit consent to the processing for one or more specified purposes;
- where the processing is necessary to carry out the obligations and exercise specific rights of Old Mission Europe or its employees;
- where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards;
- where the processing is necessary for the establishment, exercise, or defence of legal claims; and/or
- where the processing is necessary for reasons of substantial public interest, in accordance with applicable law.

Please see the table below regarding how we may use your special categories of personal information.

Further details on how we handle special category data and data relating to criminal convictions and offences are set out in our policy on processing special categories of data, and, where relevant, on criminal records data, available on request.

Information about criminal convictions

We envisage that we will process information about criminal convictions. However, we may only use information relating to criminal convictions where the law allows us to do so. This is usually where that processing is necessary to carry out our obligations and provided we do so in line with our Data Protection Policy.

We will only collect such background check information if it is appropriate given the nature of the role and where we are legally able to do so.

Where appropriate, we will collect information about your criminal convictions history if we have offered you the role or work (conditional on checks and any other conditions, such as references, being satisfactory). We may carry out a criminal records check in order to satisfy our regulatory requirement and/or that there is nothing in your criminal convictions history which makes you unsuitable for the role or work. Further background checks may be required to complete the Financial Industry Regulatory Authority (“**FINRA**”) Form U4 for UK-based personnel if they are applying for roles regulated by FINRA.

Please see the table below regarding how we may use information about criminal convictions.

Information about biometric data

Fingerprinting may be required under FINRA for UK-based personnel if they are applying for roles regulated by FINRA. If your role is regulated by FINRA, we envisage that we will process your biometric information (i.e., your fingerprint data). However, we may only use biometric information where the law allows us to do so. This is usually where that processing is necessary to carry out our obligations and provided we do so in line with our Data Protection Policy.

We will only collect biometric information if it is appropriate given the nature of the role and where we are legally able to do so.

Please see the table below regarding how we may use information about biometric data.

Automated decision-making

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

How we use your personal information

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

- Assess your skills, qualifications, and suitability for the role or work.

- Carry out background and reference checks, where applicable.
- Communicate with you about the recruitment process.
- Keep records related to our hiring processes.
- Comply with legal or regulatory requirements.

The table below sets out the categories of personal information as categorised above and how we use that information. The table also lists the legal bases on which we rely to process personal information. If you have questions about or need further information concerning the legal basis on which we collect and use your personal information, please contact the Compliance department using the contact details set out under the heading “**Contact and complaints**”, below.

Before making a final decision to recruit:

Personal data we collect	How we collect the personal data	Why we process personal data (purpose)	Legal basis for processing the personal data
• Contact information, including title, first name, last name, preferred first name, email address, physical address, and telephone/mobile number(s).	• Information you provide as part of the application process, or information from external job boards and recruitment agencies.	• To allow you to submit your application and create an account with HackerRank (if applicable), and to remain in contact throughout the recruiting process. • To provide you with the support you have requested. • To provide you with information and materials you have requested from us. • To inform the relevant manager or department of your application.	• To pursue our legitimate interests in deciding whether to appoint you to the role or for the work since it would be beneficial to our business to appoint someone to that role or for work. • To pursue your legitimate interests in receiving updates on your application/the recruitment process. • In accordance with our legitimate interest to carry out a fair recruitment process and to progress your application, arrange interviews, and inform you of the outcome at all stages.
• Details of previous education, work experience, professional qualifications and affiliations, previous projects and achievements, job title, employment history, and academic and educational background, information collected from the recruitment and hiring processes, including in your CV/resumé and cover letter, your website details, your LinkedIn profile,	• Information you provide as part of the application process, or information from external job boards and recruitment agencies.	• So that we can make an informed decision about which candidates to shortlist for interview and ultimately recruit. • To comply with legal/regulatory obligations.	• Where appropriate, to comply with our legal obligations. Otherwise in accordance with our legitimate interest to carry out a fair recruitment process; to make an informed decision to shortlist for interview and (if relevant) to recruit; and to maintain employment records and to comply with legal, regulatory, and corporate governance obligations and good employment practice.

your GitHub page, responses to questions and details in any application forms and during any interviews, letters of reference, transcripts, pre-hire interactions, and letters of offer (depending on the nature of the information this may include special category data).			
Information regarding your academic and professional qualifications.	From your education provider; from the relevant professional body.	To make an informed recruitment decision.	Legitimate interest: to verify the qualifications information provided by you.
Results of specific testing conducted by our third-party providers as part of the recruitment process.	From third-party providers we use, such as Interviewstreet, Inc. (also known as HackerRank) and other test providers.	To make an informed recruitment decision.	- To pursue our legitimate interests in deciding whether to appoint you to the role or for the work since it would be beneficial to our business to appoint someone to that role or for work. - In accordance with our legitimate interest to carry out a fair recruitment process and to progress your application, arrange interviews, and inform you of the outcome at all stages.
Details of your referees.	Information you provide as part of the application process.	- To obtain a reference about you, so that we can make an informed decision about your recruitment. - To comply with legal/regulatory obligations.	In the regulated sector, to comply with our legal obligations to obtain regulatory references. Otherwise in accordance with our legitimate interest to carry out a fair recruitment process.

• Data relating to your health <i>(depending on the nature of the information this may include special category data)</i>.	• Information you provide as part of the application process.	• To comply with our legal obligations. • To consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during a test or interview.	• To comply with our legal obligations or as is necessary for the purposes of carrying out legal rights and obligations.
--	---	---	--

After acceptance, potentially before your start date:

• PeopleCheck Limited, a background check provider, provides information on the following, as applicable: ○ Adverse media analysis and footprint ○ Professional activities ○ Education verification The following checks may be carried out after acceptance, potentially before your start date, and annually after your appointment: ○ Identification documents ○ Right to work documents (see more on immigration status below)	• Information provided from third-party sources.	• To assess your skills, qualifications, and suitability for the work or role.	• Where appropriate, to comply with our legal obligations. Otherwise in accordance with our legitimate interest to carry out a fair recruitment process; to make an informed decision to shortlist for interview and (if relevant) to recruit; and to maintain employment records and to comply with legal, regulatory, and corporate governance obligations and good employment practice.
---	--	--	--

○ Address confirmation ○ UK directorship (such as directorship search for company listings or conflicts of interest) ○ criminal records (see more on criminal records data below) ○ UK financial records (such as county court judgments, insolvencies and bankruptcy orders) ○ Alias (other known names) ○ Global sanction lists (such as global sanction check results through the Office of Foreign Assets Control) ○ FCA registry <i>(Depending on the nature of the information this may include special category data).</i>			
• Information about your previous academic and/or employment history, including details of any conduct, grievance or performance issues, appraisals, time and attendance <i>(depending on the nature of the information this</i>	• From your referees (details of whom you will have provided).	• To obtain a reference about you, so that we can make an informed decision about your recruitment. • To comply with legal/regulatory obligations.	• In the regulated sector, to comply with our legal obligations to obtain regulatory references. Otherwise in accordance with our legitimate interest to carry out a fair recruitment process.

<i>may include special category data).</i>			
Information concerning your criminal record (<i>this information is special category data</i>).	From you, provided from third-party sources and from the Disclosure and Barring Service from a criminal convictions certificate or other criminal records certificate.	- To establish your suitability for the work or role and carry out background checks. - To make an informed recruitment decision. - To perform the employment contract. - To carry out checks in accordance with our legal obligations.	Where it is necessary for compliance with a legal or regulatory (e.g., the FCA or FINRA) obligation to which we are subject (for example, where we must carry out criminal record checks for certain roles or work). Otherwise, where it is in accordance with our legitimate interest to check the suitability of staff where, although there is no legal obligation to carry out a criminal record check, it is clear from the circumstances of the work that checking is justified.
Additional information concerning your criminal record, required for those governed by FINRA (<i>this information is special category data</i>).	From you and from the Disclosure and Barring Service from a criminal records certificate or enhanced criminal records certificate.	- To establish your suitability for the work or role and carry out background checks. - To make an informed recruitment decision. - To perform the employment contract. - To carry out checks in accordance with our legal obligations.	Where it is necessary for compliance with a legal or regulatory (e.g., FINRA) obligation to which we are subject (for example, where we must carry out criminal record checks for certain roles or work). Otherwise, where it is in accordance with our legitimate interest to check the suitability of staff where, although there is no legal obligation to carry out a criminal record check, it is clear from the circumstances of the work that checking is justified.
Submission of fingerprints to FINRA for UK-based personnel if they are applying for roles regulated by FINRA (<i>this information is special category data</i>).	From you.	- To establish your suitability for the work or role and carry out background checks. - To make an informed recruitment decision.	Where it is necessary for compliance with a legal or regulatory (e.g., FINRA) obligation to which we are subject (for example, where we must carry out criminal record checks for certain roles or work). Otherwise, where it is in accordance with

		- To perform the employment contract. - To carry out checks in accordance with our legal obligations.	our legitimate interest to check the suitability of staff where, although there is no legal obligation to carry out a criminal record check, it is clear from the circumstances of the work that checking is justified.
Your immigration status, residency, citizenship, or work authorisation status, visa information, sponsorship requirement, nationality, and passport information <i>(depending on the nature of the information this may include special category data)</i>.	From you and, where necessary, the Home Office.	- To enter into/perform the employment contract. - To carry out right to work checks in accordance with our legal obligations.	To carry out obligations and exercise rights in employment law. Otherwise, where it is in accordance with our legitimate interest to maintain employment records.

Other uses of personal data:

All personal information referred to above <i>(depending on the nature of the information this may include special category data)</i>.	All information gathered.	To enable us to comply with any legal or regulatory requirements and otherwise to meet applicable requirements of any relevant regulator or competent authority.	To comply with our legal obligations. Otherwise, to pursue our legitimate interest (for the purpose of establishing, exercising, or defending our legal rights).
All personal information <i>(depending on the nature of the information this may include special category data)</i>.	All information gathered.	To exercise or protect the rights, property, or personal safety of the Company, its clients, staff, or others.	To pursue our legitimate interests in protecting the rights, property, or personal safety of the Company, its clients, staff, or others (including for the purpose of establishing, exercising, or defending our legal rights).

Who we share your information with

The above categories of personal data may be shared with other parties, such as HR consultants, professional advisers, regulators or as required to comply with the law. Usually, data will be anonymised but this may not always be possible. The recipient of the data will be bound by confidentiality obligations. In particular, your personal data may be disclosed in the following circumstances:

Transferred between Old Mission Europe and Old Mission Capital in connection with the provision of centralised IT and human resources management, business planning, budgeting, accounting, reporting, and strategy, legal and regulatory compliance and managing associated risks, providing legal advice, and in connection with potential or actual litigation, providing and administering whistleblowing schemes, and reporting, assessing, and responding to claims for risk management.

- External recruitment agents/consultants that brought your application to our attention, if applicable.
- Third-party vendors and our other partners who provide data processing services, including, but not necessarily limited to, the provider of our workplace and recruitment portals, providers which support us with communications, applicant tracking, fraud prevention, web hosting, or analytics or who otherwise process personal information for purposes that are described in this Notice or notified to you when we collect your personal information. In the event we extend an offer of employment to you, these third-party vendors or partners may also include providers of background checks associated with your employment.
- Any competent law enforcement body, regulatory body, governmental agency, court, or other third party where we believe disclosure is necessary (i) for compliance with laws or regulations, (ii) to exercise, establish, or defend our legal rights, (iii) to detect and investigate illegal or wrongful activities and/or breach of contract, (iv) to exercise or protect the rights, property, or personal safety of the Company, its clients, staff, or others, or (v) to protect your vital interests or those of any other person.
- Our insurers.
- A potential buyer (and its agents and advisers) in connection with any proposed purchase, merger, or acquisition of any part of our business. Your personal information may be disclosed to third parties in connection with a transaction, such as a merger, sale of assets or shares, reorganisation, financing, change of control, or acquisition of all or a portion of our business.
- Any other person as may be envisaged under this Notice.

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal information for

their own purposes. We only permit them to process your personal information for specified purposes and in accordance with our instructions.

Where data may be held

Data may be held at our offices and those of our group companies, third-party agencies, service providers, representatives, and agents as described above.

This Notice does not apply to third-party content, websites, or platforms. If individuals decide to provide their information to these third-party sites, they must be aware that we do not take any responsibility for their compliance with data privacy laws. Individuals are encouraged to make themselves aware of applicable privacy policies before they provide their personal information to these third-party sites.

International data transfers

As our headquarters are based in the United States, your personal information will need to be transferred to the United States for the purposes referred to under this Notice.

In addition, when we disclose your personal information with the recipients mentioned further above in this Notice, it may involve transfers of your personal information overseas, which may include transfers to countries outside of the UK/EEA whose laws provide levels of protection for personal information that are not always equivalent to the level of protection that may be provided in your own country.

We have procedures and contractual obligations in place to ensure that personal information is transferred, processed, and stored with appropriate safeguards and in accordance with applicable laws. Please contact the Compliance department using the contact details set out under the heading “**Contact and complaints**”, below, if you would like further information on the specific mechanism or protective measures we use when transferring your personal data.

If you fail to provide personal information

If you fail to provide certain 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 or work and you fail to provide us with relevant details, we will not be able to take your application further.

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.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How long we keep your data

We keep the personal data that we obtain about you during the recruitment process for no longer than is necessary for the purposes for which it is processed. How long we keep your data will depend on whether your application is successful and you become employed by us, the nature of the data concerned, and the purposes for which it is processed.

If your application is successful, we will keep only the information that is necessary in relation to your employment. For further information, see our Data Protection Privacy Notice (Employees, Workers, and Contractors).

If your application is unsuccessful at this stage, we will keep your data for the purpose of establishing, exercising and/or defending any legal claims, in accordance with our legitimate interests or for future reference in accordance with our Data Retention Policy.

Further details on our approach to data retention and destruction are available on request.

Your rights in connection with your personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information 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 information where you have exercised your right to object to processing (see below).

- **Object to processing** of your personal information 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. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

Please note that some of these rights are not absolute and there are a number of exceptions where we may not have an obligation to fulfill your request. If you want to exercise your rights in relation to your personal information, please contact the Compliance department in writing. Please note that we may ask you to provide us with additional information in order to verify your identity.

Right to withdraw consent

Where you may have provided your consent to the collection, processing, and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Compliance department. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Keeping your personal data secure

We have appropriate security measures in place to prevent personal data from being accidentally lost, used, or accessed in an unauthorised way. We limit access to your personal data to those who have a genuine business need to know it. Those processing your data will do so only in an authorised manner and are subject to a duty of confidentiality. Details of these measures may be obtained from the Compliance department.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Contact and complaints

We have appointed the Privacy team to oversee compliance with this Notice. If you have any questions about this Notice or how we handle your personal information, please contact the Privacy team at dataprotection@oldmissioncapital.com. We hope that the Privacy

team can resolve any query or concern you raise about our use of your data. If not, you may contact the Information Commissioner at <https://ico.org.uk/concerns/> or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.