

PRIVACY POLICY

1- INTRODUCTION

This Privacy Policy (the "Policy") is provided by JAR Capital (DIFC) Ltd., Registration Number 5981 and regulated by the Dubai Financial Services Authority, having its registered address at Level 16, Index Tower, Dubai International Financial Centre, Dubai, United Arab Emirates; ("JAR", the "Firm", "we", "us" or "our"). This Policy has been prepared with reference to the Data Protection Law, DIFC Law No. 5 of 2020. (the "DP Law").

We are committed to safeguarding the privacy of the personal information that we process in the course of our business, including the personal information we receive from you ("Data Subjects", "you" or "your"). This Policy describes how and why we collect, store and use personal information, and provides information about the rights of the individuals to whom such personal information relates.

JAR will be designated as a "data controller" since data submitted to us will be controlled by the Firm. We may, however in some instances, act as a "processor" (meaning that we process personal data only in accordance with the directions of a data controller, or as otherwise permitted by law).

We provide this note to inform you of our privacy policy and practices, and of the choices, you can make about what information is collected, the manner in which that information is collected and how that information is used. This Policy describes how the Firm may collect, use, store, transfer on a legal basis or otherwise process your personal data including personal data provided when using the Firm's website.

Personal data comprises all the details that the Firm collects and processes directly or indirectly about you as a Firm's website visitor, individual client or representative of a corporate client, for instance information about your identity and contact details (such as name, email id, contact number), your transactions, your financial information, interactions or dealings with the Firm, including information received from third parties and information collected through use of affiliate websites, cookies.

2- SCOPE

This Policy applies to all parties including but not limited to employees, job candidates, customers, clients, suppliers, advisors, vendors, business partners etc. who provide personal data to JAR, irrespective of the nature or amount of data disclosed to the Firm. This Policy also applies to persons anywhere in the world who access or use Firm Website Services or mobile app (or other platforms).

This Policy applies to all data including corporate data or personal data. It would, hence, apply to every server, database and IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks including any handsets from the Firm. Every user who interacts with company's IT services is also subject to this Policy. Information that is classified as 'Public' is not subject to this Policy. Other data can be excluded from the Policy by company management based on specific business needs.

3- COLLECTION OF PERSONAL INFORMATION

We may collect personal information from you in the course of our business, when you contact us, when you request us to provide you with our services, when you use our website or mobile app (or other platforms), or as a result of your relationship with any of our personnel or clients.

In general, we collect data relating to the following categories of persons:

- People who receive our services;
- Former and current employees and trainees;
- Contacts;
- Business partners;
- Service providers, suppliers, visitors to our offices and people we meet with; and
- Visitors to JAR website.

The personal information that we process includes:

- Identity data: this includes first name, last name, nationality, addresses, title, marital status, gender and date of birth, national identifiers (e.g. passport number and identity card number).
- Contact data: this includes business card, residency country, delivery address, location, billing address, email address and telephone numbers.
- Bank account and/or other financial information, if relevant to our engagement with you; this includes details of your bank account(s) and other details necessary for the purpose of providing you with our services, and for processing payments and preventing fraud. This also includes other related billing information and payment history;
- Technical information (including your location, IP address, browser details, traffic data, location data), such as information from your visits to our website or mobile app or other platforms (page interaction information, length of visits, etc.), or in relation to marketing emails we send to you;
- Anti-fraud checks data: this includes the results of any searches undertaken to ascertain whether the information provided by you is accurate;
- Information relating to your visits to our offices or our meetings and events, including appointment details (e.g. time, location, participants), CCTV images and other photographic or video images;
- Personal information provided to us by or on behalf of our clients, or generated by us in the course or providing services to them, which may include special categories of personal data;
- Employment data: this includes information about your employment. Academic and professional history data for candidates for internships, job vacancies, employees and other staff: this includes curriculum vitae and similar documentation, information relating to job titles and salaries.
- Any other information relating to you which you may provide to us.

COLLECTION OF SENSITIVE DATA

Sensitive Data is highly confidential and is collected transparently and lawfully. Such data may be processed in the Firm's ordinary course of business, such as processing personal sensitive data is

necessary for the establishment, exercise, or defense of legal rights. Prior Express Consent will be obtained before processing any such Personal Sensitive Data.

We may collect your personal information:

- As part of our new business intake and client on-boarding or client maintenance activities, and when you seek services from us, including customer due diligence and anti-money laundering compliance purposes;
- When you seek employment from us, as part of our new employee on-boarding and maintenance of the employment relationship;
- When you provide (or offer to provide) services to us, either yourself or on behalf of your employer;
- When you interact with our website or mobile app (or other platforms), or use any of our online services;
- Where you attend our events or webinars or sign-up to receive our newsletters or other marketing materials from us.

We collect data from you by way of telephone calls or other forms of virtual calls and meetings, by way of physical meetings, by way of email, post, your submission of documents and applications or other forms in soft and hard formats, or face-to-face, including in conversations with our personnel, and through your use of our website, apps or other platforms.

However, we may also collect data about you from a third party source, such as our clients, your employer, other parties to matters in which we are involved, platform operators for technology used in our business (e.g. webinar platforms), other organizations that you have dealings with, regulators or other government authorities, credit reporting agencies, information service providers, or from publicly available records.

The information you provide may be confidential, and we will maintain such confidentiality and protect your information in accordance with our professional obligations and applicable law. We have arrangements in place with personnel and service providers who may process your personal information, to ensure that confidentiality is maintained.

Our collection of data may be legally or contractually required for the provision of our services to you.

4- HOW WE USE YOUR DATA

We may use your data for the purposes set out in this Policy as well as for any legal reasons that may apply, some of which we have set out herein. We normally only process your data where required for marketing purposes and for the purpose of providing you, directly or indirectly (e.g. as a processor or on behalf of an affiliate), with our services and/or to protect our legitimate interests, or where required or allowed by law.

We are legally obliged to have a lawful reason for processing your data, which we process if:

- You have provided your consent to the processing of your data for the stated purpose;
- Processing of your data is necessary to perform or enter a contract with you (e.g. where onboarding clients, providing or administering our services, processing payments, and recruiting new employees);

- Processing is necessary to protect your vital interests or that of another natural person;
- Processing is necessary for legitimate interests pursued by us or any of our partners to whom your data was made available, except where overridden by your interests or rights; and
- Processing is required to comply with applicable law to which we are subject.

5- PURPOSE FOR PROCESSING OF PERSONAL DATA

Whether we receive your personal data directly from you or from a third party, we will only use your personal information if we have obtained your consent (where necessary), or if we have another lawful basis upon which to do so (e.g. for the performance of a contract to which you are a party, or in order to take steps at your request prior to entering into such contract; for compliance with a legal obligation on us; to protect your vital interests or those of another natural person; or for our own legitimate interests, or those of a third party, except where such interests are overridden by your own rights or interests).

The purposes for which we process your personal information include:

- Processing applications for products and/or services, including assessing customer suitability and performing necessary checks and risk assessments.
- Providing you with products and/or services, including transactions and completing instructions or requests.
- Establishing and managing investment relationships.
- Complying with our legal obligations, including with respect to legal and regulatory considerations (e.g. anti-money laundering and sanctions checks, audits, enquiries by regulatory authorities).
- Preventing, detecting, investigating and prosecuting crimes (including but not limited to money laundering, terrorism, fraud and other financial crimes) in any jurisdiction, identity verification, government sanctions screening and due diligence checks.
- Managing our business relationship with you (or your organisation), whether in connection with the provision of our services, or as your employer (or potential or former employer), including processing payments, accounting, billing and collection and related support services.
- Establishing, exercising or defending legal rights in connection with legal proceedings (including any prospective legal proceedings) and seeking professional or legal advice in relation to such legal proceedings.
- Managing and securing access to our premises and information technology systems, and monitoring the technology side of our operations.
- Keeping your contact details accurate and current using information provided by you, or information publicly available.
- Monitoring and improving our website and its content.
- Conducting market research and surveys with the aim of improving our products and services.
- Sending you information about our products and services for marketing purposes and promotions.

- For any purpose related and/or ancillary to any of the above or any other purposes for which your personal data was provided to us.

6- COOKIES

Cookies are small files aimed at enabling a website to remember who you are. Information from cookies may include information relating to your use of our websites, information about your computer (such as IP address and browser type), and demographic data. We use cookies to improve our website.

Specifically, we use Cookies to track overall site usage and to enable us to provide a better user experience. We do not use Cookies to “see” other data on your computer or determine your email address. Most internet browsers have a mechanism notifying you when you receive a new cookie, and telling you how to reject new cookies or disable cookies altogether (if you wish to do so).

Alternatively, you may wish to visit an independent source of information, www.aboutcookies.org, which contains comprehensive information on how to alter settings or delete Cookies from your computer as well as more general information about Cookies. For information on how to do this on the browser of your mobile phone you will need to refer to your handset manual or network operator for advice.

7- SHARING YOUR PERSONAL INFORMATION

Where we share your data with third parties, we always ensure appropriate measures are taken to protect your data in compliance with applicable laws.

We share your data with our affiliates, with persons representing you or arranging services on your behalf, as well as with other persons to help us provide you with our services. We also share your information where required to by law or to protect our legal rights.

In certain instances, we share your data with the following persons for the purposes set out in this Policy:

- Affiliates: JAR is a member of the JAR group of companies. Each member of the JAR group may share Personal Data with other members and affiliates in order to provide you with our services and in order to administer our relationship with you (e.g. invoicing, marketing) or otherwise as necessary for the purposes described above.
- Entities to which our services are outsourced (if any).
- Financial institutions: We share Personal Data with financial institutions in connection with invoicing and payments.
- Various external providers of professional services and of support services, i.e., such as translation, photocopying, printing and storage). The use of these services might involve the service provider receiving your relevant information from us.
- Agents, consultants, professional advisors, accountants, auditors and other outside professional advisors to JAR.

- Entities providing background check services, including credit risk, AML and CFT detection companies.
- Data protection supervisory authorities and other regulators.
- Any entity which purchases all or part of our services or Firm.
- Courts, law-enforcement authorities, regulators, public officials and other parties where reasonably necessary to establish, exercise or defend ourselves against a legal claims or to otherwise resolve legal disputes.
- Persons with whom we are permitted or obliged to share your data by applicable law;
- Law-enforcement authorities to assist them in performing their duties, including any investigations that may concern you; and
- Other public authorities where legally permissible.

8- TRANSFERRING DATA OUTSIDE THE DIFC

As part of a regional group, we deal with entities in different jurisdictions. As a result, where legally required or while carrying out our rights pursuant to this Policy, we transfer and process data inside and outside the DIFC. Certain countries where we process data may have laws less protective than those in the DIFC and the DIFC Data Protection Commissioner may consider them to not have an adequate level of data protection.

Where we transfer your data outside the DIFC, we always ensure appropriate measures are taken to protect your data in compliance with applicable laws.

Unless:

- You have expressly consented to the transfer of your data;
- The transfer of your data is necessary for us to perform the services for which we were engaged or conclude or perform a contract concluded in your interests; or
- The transfer is otherwise permitted by applicable data protection laws,

We will only transfer your data to a jurisdiction classified as adequate by the DIFC DP Commissioner or otherwise where we have put in place adequate safeguards to protect your data. In particular, if none of the above apply and we wish to transfer your data to a jurisdiction that does not have an adequate level of data protection as per the DIFC Data Protection Commissioner, we will undertake all reasonable measures to ensure this protection is set out in a written agreement between us and the receiving entity or that otherwise, the legally required measures are undertaken.

9- DATA RETENTION

We will retain your data to the extent reasonably necessary to protect our legitimate interests, comply with our legal, accounting or reporting obligations or enforce our agreements with you.

While determining the appropriate retention period of data, we take into consideration:

- Legal and contractual requirements, including how long it is reasonable to retain records to prove compliance therewith;
- Time limitations for the making of claims relating to the data;
- Mandatory or recommended record keeping obligations by laws, regulations and other advisors;
- The purposes for which we process your data;
- The nature, sensitivity and amount of the data;
- The potential risk of harm from disclosure or unauthorized use of your data; and
- Whether we can achieve our purposes through other means than retention.

10- YOUR DATA RIGHTS

Various rights may be available to you, depending on the circumstances and the applicable law. Key rights are summarized below:

- **Withdraw consent:** Where the basis to our processing of your data is consent, you have the right to withdraw such consent. Such withdrawal shall not affect the legality, accuracy and validity of any processing or related activities carried out before the date of receipt of your withdrawal;
- **Access and rectification, etc.:** you may request access to and rectification or erasure of personal information, or restriction of processing concerning the Data Subject or to object to processing as well as the right to data portability;
- **Objecting and restricting:** you may object, on legitimate grounds, to the processing of your personal information, or request that processing be restricted;

Where you wish to exercise any of the above rights, please contact us using the details set out at the end of this Policy. We may request that you confirm your identity and provide further information to enable us to assess your request.

As set out in Article 39 on the DP Law, we may not discriminate against you for exercising your rights by denying services or changing prices or quality of service, unless reasonable to do so in general, as objectively determined, and applicable to all individuals offered or receiving such benefits.

Where your request pursuant to this section is clearly groundless, repetitive or excessive, we may to the extent legally permitted, refuse to comply with your request.

11- SECURITY MEASURES

We have implemented reasonable administrative, technical and physical measures to protect your personal information against loss, misuse and alteration.

We also regularly review and update such measures to meet new perceived threats that may arise from technological advances. We cannot warrant or guarantee the security of any data you send us.

Where legally required to do so, we will notify you and any applicable regulator of any suspected or actual breach of data.

12- CHANGES TO THIS POLICY

JAR reserves the right to modify or amend this Policy at any time and for any reason. Please check back to this Policy from time to time to stay informed. It is your obligation to regularly check the Privacy Policy.

13- COMMUNICATIONS

For any inquiries or concerns regarding our Privacy Policy, or to report a complaint about how your personal data is processed:

JAR DP Contact Person:

- **Name:** Omar Nakadi
- **Email:** omar.nakadi@jarcapital.swiss
- **Phone:** +971 52 384 9500
- **Address:** Unit 1601, Index Tower (West Wing), DIFC, Dubai, UAE

Alternatively, you may reach out to:

DIFC Commissioner of Data Protection:

- **Authority:** Dubai International Financial Centre Authority
- **Office:** DIFC, Level 14, The Gate Building
- **Phone:** +971 4 362 2222
- **Email:** commissioner@dp.difc.ae