

Non-U.S. Employee Privacy Notice

In this Privacy Notice:

“Albourne Employing Company” means the company in the Albourne Group that you have signed an employment contract with.

“Albourne Group” or **“Albourne”** or **“we”** or **“us”** or **“our”** or the **“Company”** means Albourne Partners Limited and its branches and subsidiaries in existence from time to time. Albourne Group currently comprises: Albourne Partners Limited; Albourne America LLC (“AAL”); Albourne Partners (Asia) Limited; Albourne Partners Japan; Albourne Partners Deutschland AG; Albourne Partners (Singapore) Pte. Limited; Albourne Partners (Cyprus) Ltd; Albourne Cyprus Limited; Albourne Partners (Bermuda) Limited; Albourne Partners (Canada) Limited and Albourne Partners Limited, Bahrain Branch.

“Criminal Records Data” means data which may contain information about a person relating to any proceedings for any offence committed or alleged to have been committed by a person, the disposal of such proceedings or the sentence of any court in such proceedings. Data protection legislation in certain countries requires additional safeguards for the processing of Criminal Records Data.

“Data Protection Laws” means all applicable laws, rules, regulations, directives and governmental requirements relating in any way to the privacy, confidentiality, security, integrity and protection of Data, including without limitation, the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 and the GDPR, as amended or superseded from time to time, and any national implementing legislation.

“EEA” means the European Economic Area countries, namely, Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Liechtenstein, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.

“Employee” means an actual employee, an agent, an independent contractor, a secondee who has signed a contract with an Albourne Employing Company and/or officer (including directors) of any Albourne Group Company other than AAL. Examples of such individuals include job applicants, employees (temporary or permanent), contingent workers, interns, work experience students, retirees, and former employees, as well as any dependents or others of such persons.

“Employment Data” - means any Personal Data (including Special Category Data and Criminal Records Data) which is obtained in the context of an individual’s working relationship with Albourne (other than AAL) and includes Personal Data from an actual or prospective employee, an agent, an independent contractor and/or officer (including directors) of any Albourne Group Company except AAL. Examples of such individuals include job applicants, employees (temporary or permanent), contingent workers, interns, work experience students, retirees, and former employees, as well as any dependents or others whose Personal Data has been given to an Albourne Group Company by such persons.

“GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

“Home Country” - your ordinary place of residence.

“Personal Data” means any information about an identified or identifiable person; an identifiable 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 or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity.

“Special Category Data” is a subset of Personal Data which may contain information relating to a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data

concerning health¹ or data concerning a natural person's sex life or sexual orientation. Data protection legislation in certain countries requires additional safeguards for the processing of Special Category Data.

"UK" means United Kingdom.

What information Albourne collects about you and how it is collected

Albourne may collect, use, store and process your Employment Data, together with other information in the course of the recruitment process and, during your employment at Albourne. For the purposes of this Privacy Notice, "data controller", "processing" and "transferring" shall be interpreted in accordance with the GDPR. Albourne Partners Limited together with Albourne Employing Company will be data controllers of the Employment Data, which means that they are responsible for deciding how your Employment Data is held and used about you.

As part of the recruitment process and as part of your employment, Albourne will collect, store, use and disclose Employment Data in accordance with all applicable laws relating to the protection of Employment Data, including the GDPR, as amended or superseded from time to time, and any Data Protection Laws.

We collect Employment Data from you during your candidacy for a job, and during and after your employment.

We may also collect your Employment Data from various other sources and combine it with the Employment Data you provide to us. For example, we may collect your Employment Data from:

- job board websites you may use to apply for a job with us;
- providers of services that we make available to our employees as part of our benefits program;
- prior employers, when they provide us with employment references;
- professional references that you authorize us to contact;
- providers of background check, credit check, COVID 19 or other health screening services, or other screening services (where required or permitted by law);
- credentialing and licensing organizations;
- your public social media profiles or other publicly-available sources;
- employment agencies or recruiters;
- your related persons who chose to communicate with us directly;
- Company communications and IT systems/applications that automatically collect information about you, or are transmitted by you;
- third parties that you authorize to share information with us; and
- other Albourne personnel.

Such Employment Data processed by Albourne may include items of Special Category Data and Criminal Records Data processed in connection with Albourne's recruitment process and as part of your employment, including:

- **Contact information**, such as your work and home address, telephone number, email address and social media handles;
- **Identification information**, such as your social security number, government-issued identification information (e.g., driver's license, passport), photographs, or other similar identifiers;
- **Immigration status** and other information that would allow us to verify your employment eligibility such as residency, work permit status;
- **Biographical information**, such as name, date of birth, professional history, language proficiencies, professional qualifications, references, education details, information in your

- company biography, social media profiles and activity, and your photo;
- **General employment information**, such as your department, work location, job title, dates of employment, work status (e.g., full-time/part-time), work history (current, past, or prospective), timekeeping information, records of work absences, records concerning salary history, investigations, disciplinary and grievance procedures, training and learning program participation, and where permitted by law, the results of credit and criminal background checks, drug and alcohol testing/screening, health certifications (including as discussed further below), driving license number, vehicle registration and driving history, and other information reasonably necessary to administer the employment relationship with you;
 - **Special Category Data classifications**, such as your gender, nationality, ethnic origin, veteran/military status, disability, where applicable, for purposes of monitoring and promoting equal opportunity, evaluating accommodation requests regarding potential disabilities or other health conditions and/or complying with applicable laws;
 - **Compensation, benefits and payroll information**, such as salary and bonus details and history, benefits information (including information regarding health insurance, retirement savings and personal information of your spouse, minor children or other eligible dependents and beneficiaries), equity or options award information (if any), bank account information and working time records (e.g., vacation and absence records, sick leave, leave status, and hours worked);
 - **Performance information**, such as management metrics, performance evaluations and feedback, and promotion history;
 - **Expenses and travel information**, such as information about your business travel and other business expenses;
 - **Health care and medical information**, such as information related to employee participation in wellness programs, executive physicals and health insurance programs, workplace safety, and public health and government-mandated programs;
 - **Investment securities information**, such as your brokerage or other financial institution account information, including your investment securities holdings and trading activities as well as all such information for certain of your family members;
 - **Credentials and access information**, such as your Company email address, usernames, passwords, keycard number; information concerning the communications you create, store, send, and transmit using our communications equipment, networks, devices, systems and applications (e.g., voicemails, emails, time of use, files accessed, search history, web pages viewed); and information about your access to offices and facilities (e.g., keycard scans and security camera footage);
 - **Information pertaining to health screenings, vaccinations, and COVID-19**, such as whether and when you have received COVID-19 vaccines, your COVID-19 health screening results (written, verbal, physical, or electronic) – both self-reported or recorded by instrumentation, a description of whether you are experiencing or have experienced COVID-19-related symptoms (such as a fever, chills, sweats, cough, shortness of breath, sore throat, persistent sneezing or runny nose, different from allergies, difficulty breathing, fatigue, body aches, headache, new loss of smell or taste, nausea, vomiting or diarrhea) (“**COVID-19 Symptoms**”), whether and when you have tested positive or negative for COVID-19;
 - **Biometric information**, such as your fingerprint, retinal or facial scans when you use our biometric systems or company issued mobile devices;
 - **Geolocation data**, such as through your IP addresses or through company issued or approved devices;
 - **Information required for us to comply with laws**, such as the requests and directions of law enforcement authorities or court orders (e.g., child support and debt payment information); and
 - **Other information you provide to us**, such as your feedback, and survey responses where you choose to identify yourself.

How Albourne will process your personal data

Albourne will process the Employment Data it collects about you for the following purposes:

- **Workforce management.** Managing work activities and personnel generally, such as:
 - recruiting, interviewing and evaluating job candidates and employees;

- administration of payroll, wages, and other compensation;
- granting and administering equity awards, bonuses, commissions, and other incentive awards;
- administering and evaluating employee benefits, including healthcare, pensions, retirement, and savings plans and loans;
- maintaining contact details of your designated dependents and beneficiaries and communicating with them as necessary in the administration of your employee benefits and awards;
- maintaining contact details of your designated emergency contacts and communicating with them as necessary in emergencies;
- administering and evaluating vacation, paid time off, sick leave, and other leaves of absence;
- performance and compensation evaluation and promotions;
- providing training and career development opportunities;
- administering employee transfers, reassignments and secondments;
- conducting employee surveys and soliciting employee feedback;
- performing background, reference, or credit checks;
- managing disciplinary matters, grievances and terminations;
- administering business expense tracking, reimbursements, and travel;
- assisting with obtaining an immigration visa or work permit;
- maintaining a healthy workplace;
- improving our application and/or recruitment process, including improving diversity;
- accommodating disabilities or health conditions;
- providing information technology resources and support;
- maintaining internal employee directories;
- communicating with you;
- otherwise administering our employment relationship with you; and
- analyzing our workforce and information relating to any of the activities above.
- **Business operations.** Operating and managing our business, including:
 - promoting Company's services, including responding to prospective clients' requests for information;
 - ensuring equality of treatment of employees within the Albourne Group and promoting equal treatment in the asset management industry;
 - complying with Company contract requirements;
 - managing communications and IT systems;
 - research, development, and operation of our products and/or services;
 - managing and allocating Company assets and personnel;
 - implementing corporate strategy, strategic planning, project management, business continuity and succession planning;
 - maintenance of business and audit records;
 - budgeting, financial management and reporting;
 - internal communications; physical and information security; and
 - potentially evaluating and undergoing mergers, acquisitions, sales, re-organizations or disposals and integration with purchasers.
- **Compliance, health, safety, and fraud prevention.** Complying with legal and other requirements, including:
 - tax, audit, recordkeeping, reporting, verifying identity and eligibility to work, and equal opportunities monitoring requirements;
 - compliance with applicable laws, regulations, legal process, or requests by public bodies or regulators (e.g., FCA, SFC, MAS, SEC filings, judicial or administrative orders regarding individual employees such as garnishments, child support payments);
 - protecting our, your, or others' rights, health, safety, and property;
 - investigating and deterring against fraudulent, harmful, unauthorized, unethical or illegal activity, or conduct in violation of our policies or procedures;
 - implementing health and safety initiatives, including as appropriate for protecting employees and visitors, protecting vulnerable individuals, and in the interest of maintaining ongoing operations and support; and
 - pursuing legal rights and remedies, including investigating, making and defending complaints or legal claims; administering and enforcing internal policies and procedures; and sharing information with government authorities, law enforcement, courts, or private parties for the foregoing purposes.

- **Monitoring.** To protect the health, safety and security of Company's workforce, guests, property, confidential information, and intellectual property and assets and to comply with local securities laws and regulations (e.g., insider dealing laws). For example, we monitor offices and facilities, IT and communications systems, devices, equipment and applications through manual review and automated tools such as security software, website and spam filtering, and monitoring our physical premises (e.g., by using security cameras and keycard scans) to protect our, your, or others' rights, health, safety and property; operate, maintain and protect the security of our network systems and devices; protect our proprietary and confidential information and intellectual property; for recordkeeping and archiving; for personnel training and/or performance management; for the compliance, safety and fraud prevention purposes described above; to investigate and respond to security and other incidents; and for business continuity (such as monitoring business-related emails following an employee's departure).
- **Analytics.** Creating anonymous, aggregated or de-identified data that we use and share to analyze our workforce and business and for other lawful business purposes.

The above list is representative of the purposes for which Albourne collects and processes personal data of employees. Albourne may, from time to time, where required, inform you of additional uses of the personal data for other reasonable purposes. Where required by law, Albourne will ask you for your consent to the new use of your personal data.

Legal Basis for processing your personal data

Your Employment Data is collected and processed for various business purposes, in accordance with applicable laws.

Albourne will only collect, use and share your Employment Data where we are satisfied that one or more of the following legal bases apply:

- The processing is necessary for compliance with a legal obligation to which Albourne is subject, for example, disclosing information to local tax authorities, making statutory payments, avoiding unlawful termination, avoiding unlawful discrimination, meeting statutory record keeping requirements or health and safety obligations
- The processing is necessary 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 a contract, for example collecting bank details to pay your salary or processing information to provide you with the contractual benefits to which you are entitled
- The processing is based on your consent. Where consent is required for the processing in question, it will be sought from you separately to ensure that it is freely given, informed and explicit. Information regarding such processing will be provided to you at the time that consent is requested, along with the impact of not providing any such consent. You should be aware that it is not a condition or requirement of your employment to agree to any request for consent from Albourne;
- The processing is necessary for reasons of substantial public interest where such processing is proportionate to the aim pursued, respects the essence of the right to data protection and provides for suitable and specific measures to safeguard your fundamental rights and the interests;
- The processing is necessary for the legitimate interests pursued by Albourne or by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal information. Albourne considers that it has a legitimate interest in processing personal information for the purposes set out above, and to support the achievement of its immediate and long-term business goals and outcomes.

Albourne will only collect, use and share Special Category Data where we are satisfied that one or more of the following legal bases apply:

- When we have your explicit consent.
- Where we need to carry out our legal obligations or exercise our rights in connection to employment and/or
- Where it is needed in the public interest, as permitted by law.

Less commonly, we may process this data where it is needed in relation to legal claims or where it is needed to protect your interests and you are not capable of giving your consent.

Albourne will process Employment Data fairly and in accordance with Data Protection Laws. In particular, Albourne ensures that your Employment Data is:

- used lawfully, fairly and in a transparent way;
- collected only for valid purposes that Albourne has clearly explained and not used in any way that is incompatible with those purposes;
- relevant to the purposes notified to you and limited only to those purposes;
- accurate and kept up to date;
- kept only as long as necessary for the purposes Albourne has told me about; and
- kept securely.

Transfer of personal data

Employment Data held by Albourne is transferred outside of the UK, the EEA or your Home Country by reason of Albourne's global business and may be transferred to or shared amongst members from time to time of the Albourne Group within or outside the UK, the EEA or your Home Country for the purposes outlined in this Privacy Notice or to operate shared infrastructure, systems, and technology. Albourne abides by the rules on data protection on individuals and has put in place policies and procedures to safeguard your personal data. Albourne has ensured that, where a transfer of personal data to a country outside the UK, the EEA or your Home Country is necessary, the data are protected by security measures that are appropriate to the risks presented by the processing and the nature of the data.

Albourne may be required to transfer Employment Data to selected external third parties that we have hired to perform certain employment-related services on our behalf. These third parties may process the personal data in accordance with Albourne's instructions or make decisions regarding the data as part of the delivery of their services. By way of example, we may share your personal information with:

- **Company service providers.** Providers of services to the Company, such as payroll administration, benefits and wellness, human resources, occupational health, performance management, training, expense management, travel agencies, transportation and lodging, IT systems and support, information and physical security, background checks and other screenings, equity award administration, corporate banking and credit cards, health care, trade associations, insurance brokers, claims handlers and loss adjusters, and any necessary third party administrators, nominees, registrars or trustees appointed in connection with benefits plans or programs.
- **Employee service providers.** Providers of services to eligible employees as part of our employee benefits program (e.g., financial advisors, securities brokers, financial institutions and providers of health, fitness, wellness, and concierge services) who need your information to verify your eligibility and provide you with services.
- **Business transfer participants.** Parties to transactions and potential transactions whereby we sell, transfer or otherwise share some or all of our business or assets, including your personal information, such as a corporate divestiture, merger, consolidation, acquisition, reorganization or sale of assets, or in the event of bankruptcy or dissolution.
- **Professional advisors.** Accountants, auditors, lawyers, insurers, bankers, and other outside professional advisors who require your information in the course of providing their services.

Albourne may be required to disclose certain personal data to other third parties:

- **Our marketing audience.** Current and prospective clients and other business contacts with whom we share your Company biography, which may be shared on our website or in other publicly available marketing materials and communications as part of our marketing activities;
- **Government authorities, law enforcement and others.** Government authorities, law enforcement, courts, financial regulators and others as described in the compliance, health, safety, and fraud prevention section above or as a matter of law (e.g., to tax and social security authorities);
- **Clients and business partners.** Clients, other companies, and individuals with whom the Company does business or is exploring a business relationship; or

- **Other Parties** to protect its legal rights (e.g., to defend a litigation suit) or in an emergency where the health or security of an employee is endangered.

Employment Data may be transferred to and stored in a country whose laws do not provide equivalent protection to that which applies in the employee's Home Country. In such circumstances, Albourne will implement contractual or other measures to ensure an adequate level of protection for such Employment Data. Albourne and third-party suppliers will be required to comply with this Policy or to guarantee equivalent levels of protection when processing Employment Data.

Retention

Refer to Document Retention Policy on HFDB.

Right to withdraw consent

Where processing of your Personal Data is based on your consent, you have the right to withdraw your consent for processing for this purpose at any time on giving notice to Albourne by contacting Albourne HR at albourne.hr@albourne.com.

Your personal data rights

If you are resident within the UK or the EEA, under certain circumstances, you may have the right to exercise the following rights:

- **access** (the right to access the personal data Albourne holds about you);
- **rectification** (the right to have any inaccurate personal data that Albourne holds about you corrected);
- **erasure** (the right to delete your personal data where Albourne has no valid reason to continue to process it or where you have validly objected to your personal data being processed – see below);
- **objection** (the right to object to your personal data being processed where Albourne is processing such data on the basis of its legitimate interest or that of a third party);
- **restriction of processing** (the right to ask Albourne to suspend the processing of your personal data, for example, if you want Albourne to establish its accuracy or the reason for processing it);
- **portability** (the right to have your personal data transferred to you or another party).

These rights are subject to applicable legal restrictions. should you wish to exercise any of these rights or have any concerns about how Albourne handles your personal data, you may contact Albourne's Personal Data Protection Officer at dataprotection@albourne.com.

Alternatively, you may contact the applicable data protection authority, which, if you are located in

- the UK, is the Information Commissioner's Office: <https://ico.org.uk/concerns/>
- Hong Kong, is the Office of the Privacy Commissioner for Personal Data: complaints@pcpd.org.hk
- Japan, is the Personal Information Protection Commission
- in Munich, Germany is the Bavarian State Office for Data protection Supervision: [Submit an online complaint \(bayern.de\)](#)
- Singapore, is the Personal Data Protection Commission: <https://eservice.pdpc.gov.sg/case/dp>
- Cyprus, is the Office of the Commissioner for Personal Data Protection: <https://www.dataprotection.gov.cy/>
- Bermuda, is the Privacy Commissioner for Bermuda: [Contact Us | PrivComBermuda \(privacy.bm\)](#)
- Bahrain is the Personal Data Protection Authority: [Contact Us | | Kingdom Of Bahrain \(pdp.gov.bh\)](#)

Where you are not a resident in the UK or the EEA you may benefit from similar or additional protection under data protection laws in your jurisdiction. If you have received a separate privacy notice which relates to the country or state in which you are ordinarily resident ("**Your Local Privacy Notice**"), this privacy

notice shall supplement Your Local Privacy Notice and in the event of any inconsistency or conflict between Your Local Privacy Notice and this privacy notice, Your Local Privacy Notice shall prevail and govern.

Additional Notice for Employees in Bahrain

Albourne Partners Limited, Bahrain Branch is dedicated to protecting the confidentiality and privacy of information entrusted to us. We comply with Bahrain's Personal Data Protection Law No. 30 of 2018 and its implementing regulations.

This Additional Notice applies to Albourne Partners Limited, Bahrain Branch.

Your personal data protection rights

Your data protection rights are highlighted here. To submit a data request please send us an email to albourne.hr@albourne.com

- Access – You can ask us to verify whether we are processing personal data about you, and if so, to provide more specific information.
- Correction and Erasure– You can ask us to correct or erase our records if you believe they contain incorrect, outdated or incomplete information about you, or if you believe we are processing your information unlawfully
- Processing restrictions– You can ask us to temporarily restrict our processing of your personal data if you contest the accuracy of your personal data, believe that we are processing your information unlawfully, prefer to restrict its use rather than having us erase it, or need us to preserve it for you to establish, exercise, or defend a legal claim. A temporary restriction may apply while verifying whether we have overriding legitimate grounds to process it. You can ask us to inform you before we lift that temporary processing restriction.
- Objection to processing (causing harm or distress) - You have the right to object to the processing of your personal data if you believe that we are processing such data for such purpose or in that manner which causes substantial and unwarranted harm or distress to you or others, and/or if you have reasonable grounds to believe that it is likely that the processing for such purpose or in that manner will cause substantial and unwarranted harm or distress to you and others.
- Objection to processing (direct marketing) - You have the right to object to the processing of your personal data for direct marketing purposes.
- Objection to processing (Automated Individual Decision-making) – You can ask us to review any decisions made about you which we made solely based on automated processing, including profiling, that produced legal effects concerning you or similarly significantly affected you.
- Right to Withdraw Consent – You can withdraw your consent that you have previously given to one or more specified purposes to process your personal data. This will not affect the lawfulness of any processing carried out before you withdraw your consent.
- Right to lodge a complaint - You have the right to lodge a complaint with the Personal Data Protection Authority in Bahrain.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information or to exercise any of your other rights. This helps us to ensure that personal data is not disclosed to any person who has no right to receive it. No fee is required to make a request. Depending on the circumstances, we may be unable to comply with your request based on other lawful grounds. If you object to automated decision-making, we will comply with the objection unless the processing falls under any other allowable instances under the PDP Law (in which case we will inform you of said lawful basis as soon as practicable).

Data Transfers

We may transfer your personal data outside the Kingdom of Bahrain where:

- i) the recipient country has been deemed to provide an adequate level of protection by the Personal Data Protection Authority in Bahrain (see [trans-order-countries-and-territories-with-adequate-protection-en.pdf \(pdp.gov.bh\)](#));
- ii) the transfer is authorised by the Personal Data Protection Authority in Bahrain; or
- iii) the transfer is otherwise permitted by law which includes the following circumstances:
 - where the individual has consented to international transfer;
 - the transfer is necessary to perform a contract which is in the interest of the individual; and

- where necessary to protect the vital interests of the individual, to comply with a legal obligation or court order, or where necessary to defend a legal claim or with prior regulator consent.

If you have questions or comments about this Additional Notice Privacy Statement or how we administer your personal data, please direct your correspondence to: Data Protection Officer, Albourne Partners MENA. Address: Office 2976, United Tower Building 316, Road 4609, Block 346, Bahrain Bay, Manama, Bahrain or by email dataprotection@albourne.com . We aim to respond within ten (10) business days from the date we receive privacy related communications. Occasionally, it may take us longer than ten (10) days where we have a legitimate justification for doing so.