APPLICANT PRIVACY NOTICE

1. Dymon Asia Capital Ltd, its affiliates and the collective investment vehicles and client accounts which are managed or advised by Dymon Asia Capital Ltd and/or its affiliates (together, "**Dymon**", "**we**", "**us**" or "**our**") may obtain personal data about you. For the purposes of data protection law, we are a user or controller in respect of your personal data. We are responsible for ensuring that we use your personal data in compliance with applicable data protection law.

2. This notice applies if you are applying for employment with Dymon (references to "**employee**", "**employer**" and "**employment**" will be construed accordingly). Where we use the term your "**application**" in this notice, we are referring to your application to work at Dymon.

3. This notice sets out the basis on which any personal data about you will be processed by us. Please take the time to read and understand this notice.

4. As referenced in this notice, "**personal data***"* generally means any data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, Dymon (or its representatives or its service providers). In addition to factual information, it may also include any expression of opinion about an individual and any indication of the intentions of Dymon or any other person in respect of such individual.

5. **Personal data that we collect about you**

5.1 We will collect and process the following personal data about you:

a. **Information that you provide to us or one of our affiliates.** This includes information about you that you give to us by filling in forms or by communicating with us, whether face-to-face, by phone, e-mail or otherwise through the recruitment process. This information may include (but is not limited to):

i. your name, address, social security/identification number, nationality, birth date, education and qualification details, marital status, home address and home telephone number, mobile telephone number;

ii. your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation; and

iii. any other details you provide in support of your application, including (but not limited to) information contained in your CV and/or covering email and your reasons for applying to Dymon.

b. **Information we collect or generate about you**. This may include (but is not limited to):

i. work-related details such as your job position, contact details, performance at work, absences, pay and benefits information, service history, a copy of your employment agreement, passport details, photograph, health information, pregnancy and/or disability status;

ii. personal data that we collect through your communication and correspondence with us (including but not limited to your full name, email address and the content, date and time of your email correspondence); and

iii. information obtained through any interviews and assessments with you.

c. **Information we obtain from other sources**. This may include (but is not limited to) **information** relating to your credit history, your previous employment history and/or reference checks we may perform on you as part of the application or recruitment process.

6. **Special personal data that we collect about you**

6.1 Certain forms of "special personal data" are subject to specific protection or restriction by law in certain territories, including the EU. For these purposes, "special personal data" is data relating to: racial or ethnic origin; criminal activity or proceedings in certain countries; political opinions; religious philosophical beliefs; trade union membership genetic data; biometric data; data concerning health or sex life or sexual orientation. We will only process your special personal data if permitted by law and only if one of the following conditions is met (to the extent applicable):

a. you have given explicit consent in writing to the processing of the data;

b. the processing is necessary for carrying out our obligations and specific rights in the field of employment law, social security or social protection law (including obligations in relation to health and safety and disability discrimination, occupational health, sickness absence, maternity leave, family emergency leave, paternity leave, parental leave, the legality of personnel working in a particular jurisdiction, which will involve processing data in relation to nationality, work permits and visas, monitoring equality of treatment of staff, in connection with benefits including life assurance benefit, permanent health insurance, private medical insurance or pension, disciplinary action and vetting (where necessary));

c. the processing is necessary to protect your health or safety in an emergency (or that of another person) where you are physically or legally incapable of giving consent;

d. the data in question has been made public by you;

e. the processing is necessary for the purpose of, or in connection with, any actual or prospective legal proceedings, for the purpose of obtaining legal advice or otherwise for the purposes of establishing, exercising or defending legal rights subject to applicable local legislation or where courts are acting in their judicial capacity;

f. the processing is necessary for reasons of substantial public interest on the basis of local law which is proportionate to the aim pursued and which contains appropriate safeguarding measures;

g. the processing is necessary for preventative or occupational medicine;

h. the prevention or detection of crime or acts of dishonesty, malpractice or other improper conduct;

i. the processing is necessary for archiving purposes in the public interest or scientific and historical research purposes or statistical purposes; or

j. the processing is otherwise permitted by law.

In each case we will meet any additional local legal requirements and enforce any applicable duties of confidentiality vigorously, for example in relation to access to health records.

7. **Purposes**

7.1 We will process your personal data for the following purposes (to the extent applicable):

a. to process your application for employment and to ascertain whether you meet the applicable suitability standards imposed by the jurisdiction of your residence and any laws, rules, regulations, guidelines, notices or directions that apply to Dymon (including, in some cases, verifying your qualifications and references with those third parties you name);

b. to meet our legal and regulatory obligations;

c. to maintain consistent practices and procedures with respect to the collection, use, disclosure, transfer and processing of personal data across the Dymon Group worldwide. These practices and procedures include the effective recording, management and administration of personal data;

d. to maintain consistent practices and procedures with respect to the recruitment of personnel across Dymon, including the performance of human resources and other functions of Dymon;

e. equal opportunities monitoring;

f. to maintain contact with you in the future and notify you of relevant job vacancies with a member of Dymon that you might be interested in. Please note that if you do not want us to retain your information, or want us to update it at any stage, please contact us in accordance with the "How to Contact Us" section;

g. to enable service providers (such as legal, finance and accounting, information technology and human resources advisors and/or similar consultants and advisors), law enforcement or government authorities or any other third parties as required by applicable laws and regulations, to assist and render the appropriate assistance to Dymon and, where required, to further the business purpose of Dymon; and

h. to establish, exercise or defend our legal rights or for the purpose of legal proceedings.

7.2 We are entitled to use your personal data in these ways because:

a. we need to in order to take steps in preparation for entering into a contract with you, in particular to consider you for a position at Dymon;

b. we may need to in order to establish, exercise or defend our legal rights or for the purpose of legal proceedings; or

c. the use of your personal data as described may be necessary for our legitimate interests (or the legitimate interests of one or more of our affiliates), such as:

i. allowing us to effectively assess your skills, qualifications and/or the strength and merits of your application and your suitability for the role applied for;

ii. allowing us to effectively verify your information;

iii. allowing us to effectively manage the operation of our business;

iv. ensuring a consistent approach to the recruitment of our employees and the employees of our affiliates worldwide;

v. maintaining compliance with internal policies and procedures; or

vi. being able to contact you in relation to your application and the recruitment process.

8. **Disclosure**

8.1 We may share your personal data within the Dymon Group for the purposes described above and for the purposes of:

a. the management and administration of our business and our affiliates' business;

b. complying with the functions that each of them may perform relating to regional or global HR decisions;

c. the administration and maintenance of the databases storing personal data relating to our employees or to employees of our affiliates; and

d. assessing compliance with applicable laws, rules and regulations, and internal policies and procedures within Dymon.

We will take steps to ensure that the personal data is accessed only by employees of our affiliates that have a need to do so for the purposes described in this notice.

8.2 We may also share your personal data with third parties outside of the Dymon Group for the following purposes:

a. to our business partners who are contractually obliged to comply with appropriate data protection obligations;

b. assessing compliance with applicable laws, rules and regulations, as required by law of relevant government or administrative authority and then, to the extent reasonably practicable, only subject to customary undertakings of confidentiality;

c. to the extent required by law (for example, if we are under a duty to disclose your personal data in order to comply with any legal obligation), establish, exercise or defend our legal rights or for the purpose of legal proceedings;

d. to third party agents and contractors for the purposes of providing services to us, including (but not being limited to) outsourced HR service providers and consultants, IT and communications service providers, law firms, accountants and auditors. These third parties will be subject to confidentiality requirements and they will only use your personal data as described in this notice; and

e. to any organization at your request or any person acting on your behalf (including your agents, advisers, brokers and product providers).

No personal data is shared with unaffiliated third parties for their marketing purposes.

9. **International Transfers**

9.1 Personal data may be transferred internationally for the purposes described in this notice and as otherwise required or permitted by applicable law. The protections which apply to international transfers of personal data are further described in this paragraph 9 and will apply regardless of the international transfer or processing of such information.

9.2 **Transfers Outside the European Economic Area ("EEA")**

a. Where we are subject to the EU General Data Protection Regulation (or any equivalent data protection legislation) in respect of our processing of your personal data and if we transfer your personal data outside the EEA, we will ensure that it is protected in a manner that is consistent with how your personal data will be protected by us in the EEA. This can be done in a number of ways, for instance where:

i. the recipient destination has been subject to a finding from the European Commission that it ensures an adequate level of protection for the rights and freedoms that you possess in respect of your personal data;

ii. if the recipient is in the United States of America, it is a certified member of the EU-US Privacy Shield scheme; or

iii. the recipient has signed up to a contract based on "model contractual clauses" approved by the European Commission, obliging them to protect your personal data.

b. To the extent that the EU General Data Protection Regulation (or any equivalent data protection legislation) applies to you, you are entitled to request further details of the protection given to your personal data when it is transferred outside its country or jurisdiction of origin.

9.3 **Transfers Outside Singapore**. Where we are subject to the Singapore Personal Data Protection Act 2012 (No. 26 of 2012) (the "**PDPA**") in respect of our processing of your personal data and if we transfer your personal data outside Singapore, we will take all reasonable steps to ensure that:

a. the recipient agrees to protect personal data at a standard that is at least comparable to the PDPA in accordance with the PDPA; or

b. any other transfer will otherwise be in accordance with the PDPA.

9.4 **Transfers Outside Hong Kong**. Where we are subject to the Hong Kong Personal Data (Privacy) Ordinance (the "**PDPO**") in respect of our processing of your personal data and if we transfer your personal data outside Hong Kong, we will ensure that:

a. we have reasonable grounds for believing that there is in force in that recipient destination any law which is substantially similar to, or which serves the same purposes as, the PDPO;

b. you have consented in writing to the transfer;

c. we have reasonable grounds for believing that, in the circumstances in question:

i. the transfer is for the avoidance or mitigation of adverse action against you;

ii. it is not practicable to obtain your consent in writing to that transfer; and

iii. if it was practicable to obtain such consent, you would give it; or

d. we have taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that recipient destination, be collected, held, processed or used in any manner which, if that recipient destination were Hong Kong, would be a contravention of a requirement under the PDPO.

10. **Security**

10.1 Appropriate physical, electronic and procedural controls are maintained by Dymon to safeguard personal data. These standards are reasonably designed to:

a. ensure the security and confidentiality of your records and information;

b. protect against any anticipated threats or hazards to the security or integrity of your records and information; and

c. protect against unauthorized access to or use of your records or information that could result in substantial harm or inconvenience to you.

10.2 Information safeguards will be designed and implemented to control the risks identified, and the effectiveness of the safeguards' key controls, systems and procedures will be regularly tested or otherwise monitored.

a. **Access to Personal Data**. Personal data will be restricted to staff members who need to know such information with respect to the scope of their responsibilities.

b. **Information Stored in Hard Copy Formats**. Dymon has implemented and will continue to implement the following procedures to protect personal information stored in hard copy formats (to the extent practicable):

i. Personal data is kept in lockable filing cabinets.

ii. All personal data, as well as Dymon's proprietary information, is locked up at the end of each workday.

iii. Documents containing personal data is not left unattended in public spaces, such as lobbies or conference rooms.

iv. Due caution is exercised by staff members when mailing or faxing documents containing personal data to ensure that the documents are sent to the intended recipients.

v. Documents containing personal data can only be removed by staff members from Dymon's premises for legitimate business purposes. Any documents taken off premises is handled with appropriate care and returned as soon as practicable.

10.3 **Electronic Information Systems**. Dymon has implemented and will continue to implement the following procedures to protect personal data stored on electronic systems:

a. Password protection for computers, computer networks and web-based systems administered by third parties. Staff members should shut down or lock their computers when they leave the office for an extended period of time and must never share their passwords or store passwords in a place that is accessible to others.

b. Any theft or loss of electronic storage media is immediately reported to the IT Department.

c. Only authorized equipment is permitted to connect to Dymon's systems.

d. All laptops and portable storage devices containing personal data is encrypted.

e. Appropriate protections for electronic information systems, including the following:

   i. Anti-virus software

   ii. Firewalls

   iii. Prompt implementation of system patches and updates

   iv. Lock-out periods following repeated unsuccessful login attempts

   v. Monitoring of Dymon's computer systems for unauthorized use

   vi. The encryption and (where appropriate) pseudonymisation of personal data.

f. Unless otherwise advised by management, the IT Department will promptly disable system access for any terminated staff member or staff member serving garden leave.

11. **Retention**

We will retain the personal data that we obtain about you until it is no longer required in order to perform our obligations or exercise our rights under our employment agreement with you, except to the extent that we are permitted by law to retain it for a longer period of time (in which case, we will retain it for the period permitted by law) or to the extent that we may need to in order to establish, exercise or defend our legal rights or for the purpose of legal proceedings.

12. **Rights**

To the extent you are entitled to do so under applicable law:

12.1 You have a right to obtain information on, and access to, the personal data that we process about you and to request the correction of any error or inaccuracy in relation to such personal data.

12.2 You also have the following rights in respect of your personal data:

a. the right to withdraw your consent to our processing of your personal data at any time. Please note, however, that we may still be entitled to process your personal data if we can rely on another legal ground for doing so;

b. in some circumstances, the right to receive any personal data which we process about you on the basis of your consent (as opposed to any other legal ground) in a structured, commonly used and machine-readable format and/or request that we transmit such data where this is technically feasible. Please note that this right only applies to personal data which you have provided to us;

c. the right to request that we rectify your personal data if it is inaccurate or incomplete;

d. the right to request that we erase your personal data in certain circumstances. This may include (but is not limited to) circumstances in which:

   i. it is no longer necessary for us to retain your personal data for the purposes for which we collected it;

ii. we are only entitled to process your personal data with your consent, and you withdraw your consent, and where there is no other legal ground for the processing; or

iii. you object to our processing of your personal data for our legitimate interests, and our legitimate interests do not override your own interests, rights and freedom.

Notwithstanding the above, please note that there may be circumstances where you ask us to erase your personal data but we are legally entitled to retain it;

e. in some circumstances, the right to request that we restrict our processing of your personal data. This may include (but is not limited to) circumstances in which:

i. you dispute the accuracy of your personal data (but only for the period of time necessary for us to verify its accuracy);

ii. we no longer need to use the personal data except for the establishment, exercise or defence of legal claims; or

iii. you object to our processing of your personal data for our legitimate interests (but only for the period of time necessary for us to assess whether our legitimate interests override your own interests, rights and freedom).

Notwithstanding the above, please note that there may be circumstances where you object to, or ask us to restrict, our processing of your personal data but we are legally entitled to continue processing your personal data and/or to refuse that request;

f. the right not to be subject to a decision based solely on the automated processing of your personal data, where this produces legal effects concerning you or which significantly affects you; and

g. the right to lodge a complaint with the data protection regulator in your jurisdiction if you think that any of your rights have been infringed by us.

12.3 You may exercise any of the above rights or obtain further information about the use of your personal data by contacting the Chief Compliance Officer of Dymon at compliance@dymonasia.com.

12.4 In order to process your request, we reserve the right to use personal data previously obtained to verify your identity or take other actions that we believe are appropriate, subject to the requirements under applicable law.

13. Changes

If we change the way in which we process your personal data so that the information in this notice is no longer materially accurate or complete, we will update this notice and give you written notice of the change. Unless we are legally entitled to implement the change without your consent, we will seek your consent before implementing the change.

14. How to Contact Us

14.1 If you have any questions or concerns about Dymon's handling of your personal data, please contact the Chief Compliance Officer of Dymon at compliance@dymonasia.com.

14.2 In the alternative, Dymon's designated representative in the EU may be contacted using the following contact information:

Dymon Asia Capital (UK) LLP

Address: First Floor Union House, 12-16, St. Michael's Street, Oxford, OX1 2DU, United Kingdom

Email address: compliance@dymonasia.com.

14.3 We are usually able to resolve privacy questions or concerns promptly and effectively. If you are not satisfied with the response you receive from us, you may escalate concerns to the applicable privacy regulator in your jurisdiction.