

JOB APPLICANT PRIVACY NOTICE

A. General

Please review our Personal Information Collection Statement below, together with the applicable Appendix based on the country or jurisdiction in which the Barings entity you are applying to is located (the “**Relevant Country**”) (the “**Job Applicant Privacy Notice**”).

This Job Applicant Privacy Notice is provided to you in accordance with the Applicable Data Laws (as defined in the applicable Appendix), to assist you in understanding your rights and obligations in relation to the supply of personal information by you to the Barings entity (beings Barings LLC or one of its subsidiaries) that you are applying for a position with (the “**Company**”) and the manner in which the Company, acting as data controller, may use or deal with such information. Please read this Job Applicant Privacy Notice carefully.

By submitting your personal data to us, you acknowledge that the data provided:

- (a) is required for HR administration and management purposes;
- (b) may where necessary be made available to Barings’ advisers and other third parties in order to fulfil the purposes described in this Job Applicant Privacy Notice. Further because of the way Barings organizes its business, this information may be disclosed to, or processed by, other companies within the Barings Group or by other third parties engaged by Barings;
- (c) must be processed as described in this Job Applicant Privacy Notice in connection with your application and failure to supply such information will result in the Company being unable to process your employment application; and
- (d) may, where necessary, be transferred to a group company and other third parties located in a country outside the Relevant Country. In such cases, the Company will ensure that all transfers are made in accordance with this Job Application Privacy Notice.

Please note:

If your application for employment is successful, further information may also be collected from you and other sources prior to and during the period of your employment with the Company, subject to us having a legal basis to do so under the Applicable Data Laws.

B. The data we collect about you

For the purpose of processing your employment application and our consideration of your suitability for a job vacancy, and for other purposes described below we collect the following data about you:

- **Information that you provide to the Company**

This includes information that you submit to us when you make your initial application and includes:

- personal details including, but not limited to, your full name, email address, contact details, government issued ID numbers, employment history, and qualifications (both academic and professional); and
- 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 the Company.

- **Information the Company otherwise collects about you.**

This includes information that is collected in connection with your application and is likely to include:

- personal data that we collect or generate through your communication and correspondence with us (including but not limited to the content, date and time of your email correspondence); and
- information obtained or generated through any interviews and assessments with you, such as human resources data, skills and experiences, and details of qualifications.

- **Information we obtain from other sources.**

This may include:

- personal data that we collect from screening, background and/or reference checks we may perform on you as part of the application or recruitment process, which may include your address history, your credit history, your qualifications (both academic and professional), your employment history and previously held directorships (if any);
- personal data that you provide to third party organisations and where you agree to the organisation sharing your personal data with us; and
- a criminal records (where permitted under the national laws or regulations of the Relevant Country from time to time) or background check.

C. Use of your personal data

The purposes for which personal information relating to employees and potential employees may be used by the Company are as follows:

	Purpose	Legal Basis for Processing
1	Processing your employment applications, including checking references and carrying out background checks via a third-party employment background check provider.	<ul style="list-style-type: none"> • The entering into / performance of a contract with you (if applicable in your jurisdiction). • The Company's legitimate interest regarding the process for the recruitment of employees. • Compliance with legal and regulatory obligations.
2	Communicating with you regarding your candidacy for employment.	The Company's legitimate interest regarding the process for the recruitment of employees.
3	Reviewing salaries, bonuses and other benefits.	The Company's legitimate interest to analyze remuneration packages for its personnel.
4	Consideration for your suitability for a job vacancy, promotion, training, secondment or transfer.	<ul style="list-style-type: none"> ○ The Company's legitimate interest for managing recruitment; ○ In the event of a successful hiring process, the performance of your employment contract (if applicable in your jurisdiction) and/or the Company's legitimate interests in relation to career planning; and

		<ul style="list-style-type: none"> o In relation to training, the Company's legitimate interest to organize training for its employees.
5	Providing employee references.	The legitimate interest of the person requesting the reference in ensuring an efficient recruitment process.
6	Arranging any other activities in connection with employment and business of the Company e.g. medical cover, retirement scheme.	The performance of the contract in order to provide benefits to its employees or the Company's legitimate interest to manage its business.
7	Performing its functions as employer or actions necessary to the discharge of such functions. In the course of performing its functions, the Company may, as permitted by law, transfer or exchange data provided by you with data held, or hereafter obtained, for these or any other purposes by the Company, to government bodies and other regulatory authorities, corporations, organizations or individuals in the Relevant Country or otherwise overseas for the purpose of verifying that data.	The fulfilment of the Company's legal obligations to reply to requests from supervisory authorities or other competent public bodies.
8	Filing with relevant parties in the Relevant Country and overseas as required (e.g. relevant regulatory bodies).	Compliance with the Company's legal obligations.
9	Meeting the disclosure and compliance requirements under any laws or regulatory requirements applicable to the Company or any of its affiliates in the Relevant Country or elsewhere from time to time.	Compliance with the Company's legal obligations.
10	Publishing of internal directories, when necessary.	In order to meet the Company's legitimate interests in managing the professional activities of its staff.
11	Organization and management of mergers, acquisitions, sales, reorganizations and disposals of the Company's activities.	In order to meet the Company's legitimate interest in ensuring the development and transfer of its assets.

Please note: if your application is successful and you are subsequently offered and accept employment at the Company, the information we collect during the application and recruitment process will become part of your employment record.

D. Processing / disclosure of your information by / to processors / third parties

Personal information held by the Company relating to employment applicants and employees will be kept confidential but the Company may provide such information to:

- any agent, contractor, or third party service provider who provides services to the Company in connection with the operation of its business and human resources management or any of the purposes described in this Job Applicant Privacy Notice. Any such third party will be required to keep the information confidential;
- head office of the Company or any group company;
- persons from whom we seek references; and
any government bodies, other regulatory authorities, corporations, organizations or individuals in the Relevant Country and/or overseas for compliance with law or regulation, or a court or administrative order having force of law.

As noted above, some of these recipients may be located outside of the Relevant Country, as the Company is part of a global entity with offices and suppliers in various locations throughout the world. In such cases, the Company will ensure that the processing of your personal information is made in accordance with this Job Application Privacy Notice.

E. Retention of personal data

Personal information collected may be maintained for such period as may be:

- permitted by the national laws or regulations of the Relevant Country from time to time;
- required under Applicable Data Laws (as defined in the applicable Appendix); or
- as otherwise needed to fulfil any of the purposes set out in Section C above.

In some instances, based on the legitimate interests of the Company, where we may retain your information to consider you for other roles and future opportunities at the Company which may be of interest to you.

F. Your rights

Under and in accordance with the terms of the Applicable Data Laws, you may have certain rights in relation to your information, including the right to:

- request access to, correct any inaccuracies in, and in certain circumstances, request erasure, or object to or restrict the use, of your personal data, and object to certain uses or other processing of your personal data (including automated processing), in each case subject to the conditions and/or restrictions set out in Applicable Data Laws;
- in limited circumstances, data portability in respect of certain personal data, which means you can request that the Company provide a copy of your disclosable personal data to you or a third party nominee;
- lodge a complaint with the Company that is the data controller and/or with a relevant supervisory authority about the processing of your personal data by the Company;
- request that we erase your personal data in certain circumstances. Please note that there may be circumstances where you ask us to erase your personal data but we are legally entitled to retain it; and

- request that the Company correct any personal information relating to you which is inaccurate, out-of-date, incomplete, irrelevant or misleading.

Subject to the terms of the Applicable Data Laws (as defined in the applicable Appendix), the Company may charge a reasonable fee for the processing of any such request.

To exercise any of these rights, please send confirmation of your request as directed in the applicable Appendix and providing any relevant identifying information.

G. Complaints

If you would like to contact us in relation to how your personal data is handled, please contact the relevant Barings Data Privacy Manager as set out in the applicable Appendix and your complaint will be handled in accordance with our handling procedures. You may also have the right to make a complaint with the applicable local supervisory authority in the Relevant Country; however, we would request in the first instance you contact us.

Please see the applicable Appendices attached to this Job Applicant Privacy Notice for contact details in respect of each Relevant Country.

H. Security

The Company has put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way. Additionally, the Company limits access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

The Company has put in place procedures to deal with any suspected personal data security breach and will notify you and any applicable regulator of a suspected breach where the Company is legally required to do so.

I. Self-Identification Information

Where permitted under the national laws or regulations of the Relevant Country from time to time, we will ask you to complete our Self-Identification Form (the “**Form**”). Please review the information provided below so that you understand the purpose of the Form and the use of data collected through it. By providing data through the Form you consent to the use of the data you submit for the purposes described below.

Note that completing the Form is voluntary*

- **What is the purpose of the Form?**

The Company aims to have an inclusive environment for all employees by identifying and removing barriers in our practices. To help us gather a full picture of the diversity of people working at, or applying for positions at the Company, you have an opportunity to disclose certain demographic data. You will be asked to provide information about race/ethnicity, gender, and whether you identify as a member of the LGBTQ+ community (some of this data is ‘special category data’ under the Applicable Data Laws (as defined in the applicable Appendix). Providing this demographic data will help the Company build an inclusive environment, evaluate

progress toward the firm's overall diversity, equity and inclusion initiatives and goals, and measure impact and outcomes for varying groups at all stages of the employee life cycle. It will help the Company to respond (on an anonymized basis) to requests for information from Barings' clients, who are increasingly focused on Barings' progress towards its own diversity and equity goals. It will also help Barings meet its obligations under any applicable laws or regulations relating to the protection of employees from discrimination in the work place and society (as may be identified in the Self Identification Information document found on [Barings Privacy Notice Webpage](#)).

- **How will the Company handle any information which is voluntarily shared through the Self-Identification Form?**

Your responses are confidential, and the Company will comply with all Applicable Data Laws. Within the Company, those who will have access to this data include personnel in the Human Resources, Legal and Compliance departments (and other support functions (as may be necessary)) that are responsible for processing, evaluating and monitoring data.

Anonymized data may be shared with the Company's leadership and external organizations for the purposes of equality charters, initiatives and resolutions and/or responding to request for proposals (RFP) and due diligence questionnaires (DDQ); and (b) the information can also be included in reports that assess progress toward goals and/or commitments that the Company has made. The reports will not name individuals and published information will be aggregated.

****Please Note: Completing the Form is entirely voluntary and does not affect your employment or potential employment in any way. However, we hope you decide to complete it, as it will help to assist the Company in its efforts to create a diverse, equitable and inclusive environment. You may freely decide to give or refuse your consent. If you decide to complete this Form, you remain entitled to withdraw your consent to our use of the data provided at any time and without providing a reason. If you decide not to complete the Form or withdraw your consent, this will not have any negative impact on your employment or potential employment with the Company, nor will it be used to your detriment in any regard. In case of withdrawal of your consent, the data you provided in the Form will no longer be processed (except for compliance with our applicable regulatory and / or statutory obligations). You may withdraw your Form by e-mailing the Barings Global Data Privacy Manager at DPM@Barings.com.***

This Job Applicant Privacy Notice was prepared on August [], 2022 and the Company reserves the right to amend and update the notice and related appendices at any time.

Please see the applicable Appendices attached to this Job Applicant Privacy Notice for exceptions to filling out the "Form" in each Relevant Country.

Local Appendices

Applicants agree to the Job Applicant Privacy Notice and any county-specific appendices when submitting their application.

[APPENDIX A - United Kingdom & the European Union \(Ireland, Spain, Germany, Netherlands, Italy, Sweden, Denmark\)](#)

[APPENDIX B – United States of America](#)

[APPENDIX C – Australia](#)

[APPENDIX D – Peoples Republic of China](#)

[APPENDIX E – Hong Kong S.A.R.](#)

[APPENDIX F – Japan](#)

[APPENDIX G – South Korea](#)

[APPENDIX H – Singapore](#)

[APPENDIX I - Switzerland](#)

[APPENDIX J - Taiwan](#)

[APPENDIX K - DIFC](#)

APPENDIX A – United Kingdom & the European Union

This Appendix A shall be applicable to all candidates applying for a position at a Barings entity located within the United Kingdom or the European Union.

In the event of any conflict or inconsistency with the main body of the Job Applicant Privacy Notice, this Appendix A shall prevail.

Applicable Data Laws

For the purposes of this Appendix A, Applicable Data Laws shall mean any applicable data protection laws relating to the protection of individuals with regards to the processing of personal data in the relevant jurisdiction, including, as applicable:

- (a) the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") (together with any laws implemented by EU member states (including any replacement legislation applicable in the United Kingdom, whether or not as a result of any full or partial departure of the United Kingdom from the European Union), which contain derogations from, or exemptions or authorisations for the purposes of, the GDPR, or which are otherwise intended to supplement the GDPR);
- (b) the French Data Protection Law n° 78-17 dated January 6, 1978;
- (c) the Italian Legislative Decree 196/2003 (Italian Privacy Code);
- (d) the UK Data Protection Act 2018; and
- (e) any corresponding or equivalent UK or EU national laws or regulations relating to the collection, use, disclosure and processing of personal data including any amendment, update, modification to or re-enactment of such laws and guides and codes of practice issued from time to time by any supervisory authorities, in each case as amended, updated or replaced from time to time.

International Transfers

Subject to the Applicable Data Laws, transfers to other countries or jurisdictions outside of the UK or EEA may be permitted where such transfer is made to jurisdictions or countries providing "adequate protection" for personal data, including to our related entities or third-party service providers in the following jurisdictions: United States, Hong Kong, Singapore, Japan, Korea, and Taiwan.

However, some transfers may be to countries or jurisdictions that do not have adequate protection and, in that case, the Company shall conduct the transfer in accordance with the transfer requirements set out in the Applicable Data Laws such as by putting in place European Commission or UK Government approved "Standard Contractual Clauses" and by adopting appropriate supplementary measures necessary to bring the level of protection of the personal data undergoing transfer up to a level of protection equivalent to that within the EU/EEA and UK. You can request a copy of the measures applying to the transfer of personal data by using the contact information as stated below.

Complaints

If you believe that your privacy has been breached, please contact us using the details below and provide details of the incident so that we can investigate and respond to you about your concerns. We will review all communications and complaints submitted to us in this manner and will aim to respond to you in writing within a reasonable time. Notwithstanding the above, you have the right to make a complaint at any time

to the Information Commissioner's Office (ICO), the UK supervisory authority, or to any other data protection agency in the country in which you are applying for a position.

Contact Us

To contact us in relation to the Job Applicant Privacy Notice, please use the following methods:

E-mail: DPM@Barings.com

Barings Data Privacy Manager

Baring Asset Management Limited

20 Old Bailey

London, UK

French law amendments

Regarding data subjects rights, the French Data protection Act of 1978 provides a specific right to give instructions regarding the processing of data subject's data after his/her death.

APPENDIX B - UNITED STATES OF AMERICA

This Appendix B shall be applicable to all candidates applying for a position at a Barings entity located within the US.

In the event of any conflict or inconsistency with the main body of the Job Applicant Privacy Notice, this Appendix B shall prevail.

Applicable Data Laws

This Job Applicant Privacy Notice provides you with certain information that must be provided in accordance the:

- Federal Trade Commission Act (15 U.S.C. §§ 41 to 58) (“FTC Act”);
- Financial Services Modernization Act (15 U.S.C. §§ 6801 to 6827) (Gramm-Leach-Bliley Act) (“GLBA”);
- Health Insurance Portability and Accountability Act of 1996 ([Pub. L. No. 104-191](#)) (“HIPAA”); and
- California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 to 1798.199) (“CCPA”),

and for the purposes of this Appendix B are together the “Applicable Data Laws”.

In accordance with the Applicable Data Laws, you consent to Barings collecting, processing, transferring and storing the personal data including sensitive personal data contained in this Job Applicant Privacy Notice

A. CALIFORNIA

Under the CCPA, the Company is required to provide California residents with specific information about our personal information practices. The CCPA defines the term “personal information as “information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. “

Categories of Personal Information that We Collect, Disclose, and Sell

We do not sell any of your personal information for monetary compensation or other valuable consideration.

We currently do not share your information with non-affiliated third parties for their own marketing purposes. We collect and disclose certain personal information in the course of our business as described in the Job Application Privacy Notice.

Notification related to Collection of Vaccination Information

In the United States, the Company may collect information about our employees’ vaccination status, including whether they are vaccinated, the vaccine manufacturer and dates of when the vaccine was received (including the dates of any booster(s)). The Company uses vaccination information to help provide a safe environment for its employees and as may be necessary to comply with any obligations under applicable law. The Company may also use this information to determine office access and attendance at events. The Company uses vaccination information only for the purposes described in this Appendix B. The Company reserves the right to use and disclose our employees’ aggregate, de-identified information

for any lawful purpose. However, the Company will not use or share employees' vaccination information for any marketing, advertising or commercial purposes.

California Resident Rights

California law grants California residents certain rights and imposes restrictions on particular business practices. We are required to provide you with a notice about our information collection practices at or before the point of collection; to this end, there may be circumstances in which we provide an additional notice to you. California residents have the right to opt-out of our sale of their personal information. Subject to certain exceptions, California residents have the right to (at no charge) request that we (1) delete the personal information that we hold about them, subject to certain exceptions and (2) send a copy of the specific pieces of personal information that we have collected about them in the prior 12 months and to have this delivered, free of charge, either (a) by mail or (b) electronically in a portable and, to the extent technically feasible, readily useable and transferrable format. California residents also have the right to request that we provide them certain information about how we have handled their personal information in the prior 12 months, including the:

- categories of personal information collected;
- categories of sources of personal information;
- business and/or commercial purposes for collecting and selling their personal information;
- categories of third parties/with whom we have disclosed or shared their personal information;
- categories of personal information that we have disclosed or shared with a third party for a business purpose; and
- categories of third parties to whom the residents' personal information has been sold and the specific categories of personal information sold to each category of third party.

California residents may make Requests to Know up to twice every 12 months. The CCPA prohibits discrimination against California residents for exercising their rights under the CCPA. Discrimination may exist where a business denies or provides a different level or quality of goods or services, or charges (or suggests that it will charge) different prices, rates, or penalties on residents who exercise their CCPA rights, unless doing so is reasonably related to the value provided to the business by the residents' data.

CONTACT US

To contact us in relation to the Job Application Privacy Notice, including Requests to Opt-Out of Sale of Personal Information (if applicable), Requests to Know, and Requests to Delete, please use the following methods:

Electronically: Submitting a CCPA Webform found at <https://www.barings.com/guest/content/ccpa-request>

By Phone: 1-877-766-0014 (toll free)

E-mail: DPM@Barings.com

Barings Data Privacy Manager

20 Old Bailey, EC4MBF

London, UK

We will respond to verifiable requests received from California consumers as required by law.

I hereby confirm and acknowledge that I have read and understood this Job Applicant Privacy Notice before furnishing to the Company personal information relating to myself and/or other persons. I consent to the use of such personal information and all personal information previously supplied, if any, by the Company for the purposes of discharging all or any of its functions described in this Job Applicant Privacy Notice and/or the Privacy Notice and for any other purpose directly related to those purposes.

APPENDIX C - AUSTRALIA

This Appendix C shall be applicable to all candidates applying for a position at a Barings entity located within Australia.

In the event of any conflict or inconsistency with the main body of the Job Applicant Privacy Notice, this Appendix C shall prevail.

Applicable Data Laws

For the purposes of this Appendix C, Applicable Data Laws shall mean any applicable data protection laws relating to the protection of individuals with regards to the processing of personal data, including:

- (a) *Privacy Act 1988* (Cth);
- (b) Australian Privacy Principles (“APP”) as set out in the *Privacy Act 1988* (Cth); and
- (c) any corresponding or equivalent national laws or regulations relating to the collection, use, disclosure and processing of personal data including any amendment, update, modification to or re-enactment of such laws and guides and codes of practice issued from time to time by any supervisory authorities, in each case as amended, updated or replaced from time to time.

Collection Of Personal Data

In some circumstances, we may need to collect additional personal data from you, or collect personal data from you in a way which is not described in the Job Applicant Privacy Notice. Where this is the case, we will provide you with additional information which details the personal data we will collect from you and how we will use, hold and disclose that Personal data.

Security

We store your personal data in different ways, including in paper and in electronic form. The security of your personal data is important to us. We take all reasonable measures to ensure that your personal data is stored safely to protect it from interference, misuse, loss, unauthorised access, modification or disclosure, including electronic and physical security measures.

How To Access Your Personal Information?

You may contact us using the details below if you wish to find out about the personal data we hold about you. We may need to verify your identity before giving you access.

In certain circumstances, we may not be able to tell you what personal data is held about you. In these circumstances, we will notify you to explain why we cannot provide the information and attempt to find alternative means to enable you to access your information.

How To Request Correction Of Your Information?

If you believe that the personal data the Company holds about you is inaccurate, incomplete or out of date, you should contact us using the details below. We will promptly update any personal data that we consider is inaccurate, incomplete or out of date. If we do not agree that your information is inaccurate, incomplete or out of date, we will notify you and provide you with the reasons.

International Transfers

We are likely to disclose or store your personal data outside of Australia. We may disclose your personal data (including to our related entities or third-party service providers) in the following jurisdictions: United Kingdom, European Union, United States, Hong Kong, Singapore, Japan, Korea, and Taiwan.

Complaints

If you believe that your privacy has been breached, please contact us using the details below and provide details of the incident so that we can investigate and respond to you about your concerns.

We will review all communications and complaints submitted to us in this manner and will aim to respond to you in writing within a reasonable time. If your complaint is not satisfactorily resolved, you may access an external dispute resolution service or apply to the Office of the Australian Information Commissioner (“**OAIC**”) to have the complaint heard and determined. When we notify you about our decision, we will explain how you may access an external dispute resolution scheme or make a complaint to the OAIC.

Contact

Us

To contact us in relation to the Privacy Notice, please use the following methods:

E-mail: DPM@Barings.com

Barings Data Privacy Manager

20 Old Bailey, EC4MBF

London, UK

APPENDIX D – PEOPLES REPUBLIC OF CHINA

This Appendix D shall be applicable to all candidates applying for a position at a Barings entity located within the People's Republic of China (excluding for the purposes of this Appendix D Hong Kong S.A.R., Macau S.A.R. and Taiwan)

Please take the time to read and understand this Appendix D together with the Job Applicant Privacy Notice carefully. Please indicate your consent and separate consent to certain processing of your personal data as set out under this Appendix D by ticking the relevant boxes

In the event of any conflict or inconsistency with the main body of the Job Applicant Privacy Notice, this Appendix D shall prevail.

Applicable Data Laws

For the purposes of this Appendix D, Applicable Data Laws shall mean any applicable data protection laws relating to the protection of individuals with regards to the processing of personal data, including:

- (a) Personal Information Protection Law of the People's Republic of China 2021; and
- (b) any corresponding or equivalent laws, administrative regulations, sectoral rules, regional regulations, and national or industrial standards relating to the collection, use, disclosure and processing of personal data including any amendment, update, modification to or re-enactment of such laws and regulations and standards issued from time to time by any supervisory authorities, in each case as amended, updated or replaced from time to time

Additional Personal Data Collection

As required by applicable law, we may need to collect additional personal data from you, including without limitation to:

- (a) your identification document, visa, work permit or residence permit, for the purpose of performing our statutory obligations as a potential employer;
- (b) your body temperature, nucleic acid test results, vaccination status, health declaration and recent travel history, for the purpose of complying with applicable pandemic control measures.

Sensitive Personal Data

Sensitive personal data means any personal data that once leaked or illegally used, is likely to cause harm to the personal dignity of the relevant individual or potentially endangers the physical and property safety of the individual, including biometric data, religious belief, special identity, medical/health data, financial

account information and location tracking data, etc. and personal information of minors under the age of 14.

We need to process your sensitive personal data, such as your work or residence permit, credit history, criminal records, health information, etc. in order to perform our statutory duties and obligations including but not limited to those imposed on regulated fund managers.

We will only process your sensitive personal data with your separate consent and in strict compliance with the Applicable Data Laws. Please note that if you do not consent to our processing of such sensitive personal data, we may not be able to perform our statutory obligations and consider your job application.

International Transfer

Subject to the Applicable Data Laws, transfers of your personal data out of mainland China may be permitted where you have given your separate informed consent to such transfers.

You may find a list of Barings group companies which may receive your personal data through this [link](#). In addition, we may share your personal data with third party service providers located outside of mainland China which process your personal data on behalf of Barings. Details of such overseas third party service providers are set out in the below table.

Recipient name	Contact Details	Purpose of processing	Manner of processing	Types of personal information to be shared
HireRight	Phone: 864008424212 Email: customerservice.apac@hireright.com	Background Check	HireRight will use the email address provided by Barings to send a form to collect background history and further personal information required for the background check. Information provided directly to HireRight in the form will be stored in HireRight's system.	email, first name, last name

If we transfer any of your personal data outside of mainland China, we will ensure that the recipient of your personal data complies with the protection standards set out in the Applicable Data Laws.

Your Rights

In addition to the rights set out in the main body of the Job Applicant Privacy Notice, you are also entitled to the following rights in accordance with the Applicable Data Laws:

- (a) the right to request further explanation of our processing of your personal data; and
- (b) the right to withdraw your consent to the processing of your personal data at any time. If you withdraw your consent, it will not affect the effectiveness of our processing activities based on your consent before the withdrawal. However, please note that in some cases, even if you withdraw your consent, we may still have the right to process your personal data based on other legal grounds.

Contact Details

To contact us in relation to the Job Application Privacy Notice, please use the following methods:

E-mail: DPM@Barings.com

Barings Data Privacy Manager

20 Old Bailey, EC4MBF

London, UK

APPENDIX E – HONG KONG S.A.R.

This Appendix E shall be applicable to all candidates applying for a position at a Barings entity located within Hong Kong.

In the event of any conflict or inconsistency with the main body of the Job Applicant Privacy Notice, this Appendix E shall prevail.

Applicable Data Laws

For the purposes of this Appendix E, Applicable Data Laws shall mean any applicable data protection laws relating to the protection of individuals with regards to the processing of personal data, including:

- (a) Personal Data (Privacy) Ordinance (Cap. 486); and
- (b) any corresponding or equivalent laws or regulations applicable in Hong Kong S.A.R. relating to the collection, use, disclosure or processing of personal data including any amendment, update, modification to or re-enactment of such laws and guides and codes of practice issued from time to time by any supervisory authorities, in each case as amended, updated or replaced from time to time.

Contact Details

To contact us in relation to the Privacy Notice, please use the following methods:

E-mail: DPM@Barings.com

Barings Data Privacy Manager

20 Old Bailey, EC4MBF

London, UK

APPENDIX F - JAPAN

This Appendix F shall be applicable to all candidates applying for a position at a Barings entity located within the Japan.

In the event of any conflict or inconsistency with the main body of the Job Applicant Privacy Notice, this Appendix F shall prevail.

Applicable Data Laws

For the purposes of this Appendix F, Applicable Data Laws shall mean any applicable data protection laws relating to the protection of individuals with regards to the processing of personal data, including:

- (a) Act on the Protection of Personal Information (“**APPI**”)(as amended); and
- (b) any corresponding or equivalent national laws or regulations relating to the collection, use, disclosure and processing of personal data including any amendment, update, modification to or re-enactment of such laws and guides and codes of practice issued from time to time by any supervisory authorities, in each case as amended, updated or replaced from time to time.

Transfer of Personal Data to a Third Party

You hereby consent to transfer or disclosure of your personal information to a third party as provided in Section D. The Company may transfer your personal information without your consent only where such transfer without your consent is in compliance with APPI.

International Transfers

Subject to the Applicable Data Laws, transfers to other countries or jurisdictions outside of Japan may be permitted where such transfer is made to jurisdictions or countries that have been “white-listed” by the Personal Information Protection Commission (“PPC”) under the APPI or the third party receiving personal data has established similarly adequate standards for privacy protection as specified in the enforcement rules of the APPI (which includes the UK and EU countries).

However, some transfers may be to countries or jurisdictions that do not have similarly adequate standards for privacy protection and have not been “white-listed” by PP. In this case, the Company will transfer your personal data to those jurisdictions or countries only where:

- the Company provides the following information to you and you give consent to the transfer of your personal data to such countries with the following information:
 - name of the country where the receiving party resides;
 - data protection law system in the country; and
 - the data protection measures that the receiving party implements,

For the avoidance of doubt, the Company may transfer your personal data to:

- (a) third parties located in the United States of America, who will be governed by the Applicable Data Laws set out in Appendix B and subject to an appropriate data processing agreement; and / or
- (b) any other Barings entities, located in [Australia, the People’s Republic of China, Hong Kong S.A.R., South Korea, Singapore, Taiwan, and the United States of America] who will be governed by the Applicable Data Laws set out in the relevant Appendix and subject to an intra-group data privacy agreement,

as may be necessary for the purposes set out in the main body of the Job Applicant Privacy Notice; and

- The receiving party is legally obligated, such as by a data processing agreement or an intra-group data protection policy, to provide security measures ensuring data protection equivalent to or greater than that provided in the APPI.

Contact Details

To contact us in relation to the Privacy Notice, please use the following methods:

Hiroataka Norita – Head of Compliance, Japan

E-mail: Hiroataka.Norita@barings.com

Baring Japan Limited
7F Kyobashi Edogrand
2-2-1 Kyobashi
Chuo-ku
Tokyo 104-0031, Japan

APPENDIX G – SOUTH KOREA

This Appendix G shall be applicable to all candidates applying for a position at a Barings entity located within South Korea.

In the event of any conflict or inconsistency with the main body of the Job Applicant Privacy Notice, this Appendix G shall prevail.

Applicable Data Law

For the purposes of this Appendix G, Applicable Data Laws shall mean any applicable data protection laws relating to the protection of individuals with regards to the processing of personal data, including:

- (a) the Personal Information Protection Act (“PIPA”);
- (b) Protection of Credit Information Act (“Credit Information Act”);
- (c) Protection of Communications Secrets Act;
- (d) Act on the Lapse of Criminal Sentences; and
- (e) any corresponding or equivalent national laws or regulations relating to the collection, use, disclosure and processing of personal data including any amendment, update, modification to or re-enactment of such laws and guides and codes of practice issued from time to time by any supervisory authorities, in each case as amended, updated or replaced from time to time.

Collection Of Personal Data

We obtain your consent when collecting and using your personal data unless such collection and usage is based on the PIPA, the Credit Information Act, or other laws or regulations of Korea.

Special Category Data

Under the PIPA, information on the ideology, creed, membership of a labor union or political party, political views, health, sexual preferences, genetic information, information on an individual's physical, physiological, and behavioural characteristics generated through certain technical means for the purpose of identifying a specific individual (i.e., bio-data), racial/ethnic data and criminal records as defined under the Act on the Lapse of Criminal Sentences is considered “Special Category Data” for the purposes of this Appendix K.

When collecting Special Category Data from you, we comply with all the procedures and methods stipulated by the PIPA, including obtaining your separate consent for the processing of Special Category Data.

Outsourcing Of The Processing Of Personal Data

Please see below the list of third-party processors (“Processors”) together with the specific processing tasks to be outsourced. The personal data transferred to the Processors will be retained only to the extent necessary for the purposes of the services provided and to meet any regulatory requirements in accordance with any applicable laws.

We comply with all the relevant laws and regulations when outsourcing the processing of personal data. For example, we do not outsource the processing of Particular Identification Data as defined under the

PIPA (i.e., resident registration numbers (“RRNs”), driver’s license numbers, passport numbers, and alien registration numbers) to Processors located outside of Korea.

Name of the third-party processor	Outsourced task/service
NAVEX Global, Inc.	Operation of Barings’ ethics and whistle-blower hotline

Provision Of Personal Data To Third Parties

Subject to your separate consent, the following personal data may also be disclosed to third parties, i.e., independent data controllers as set out below.

We comply with all the relevant laws and regulations when providing personal data to a third party. For example, we do not provide Particular Identification Data as defined under the PIPA to recipients located outside of Korea.

Recipient	Recipient’s Purpose of Use	Transferred Items	Recipient’s Period of Retention and Use
Barings LLC	Regulatory, risk and compliance oversight	Anonymized data to perform regulatory, risk and compliance oversight	7 years from the date of collection
Baring Asset Management	Limited Regulatory, risk and compliance oversight	Anonymized data to perform regulatory, risk and compliance oversight	7 years from the date of collection

Data Protection Officer

The data protection officer is Ho Chul Jung (정호철) and is available at +82 2 3788 0529 or via e-mail at Hochul.jung@barings.com.

Measures To Ensure Security Of Personal Data

We take the following technical, managerial and physical measures necessary to ensure the security of your personal data.

Managerial measures: Designation of a data protection officer, establishment and implementation of an internal management plan, regular training of employees on personal data protection, etc.

Technical measures: Management of the right to access the personal data processing system, installation of an access control system, encryption of Particular Identification Data (as defined under the PIPA), installation of security programs, etc.

Physical measures: Restriction on access to personal data storage mediums such as the computer room and data storage room, etc.

Process and Method for Destroying Personal Data

The process and method for destroying personal data are set forth below.

- We select the relevant personal data to be destroyed and destroy it with the approval of our data protection manager using the latest approved deletion process
- We destroy personal data recorded and stored in the form of electronic files by using a technical method (e.g., low level format) to ensure that the records cannot be reproduced, and personal data recorded and stored in the form of paper documents will be shredded or incinerated.

Retention of Personal Data

In connection with Section E of this Job Applicant Privacy Notice, if we are required to retain your personal data in accordance with Applicable Data Laws, we will do so for the following purposes and periods as required by Applicable Data Laws:

- Records of logins and IP addresses used: 3 months (Protection of Communications Secrets Act)

APPENDIX H - SINGAPORE

This Appendix H shall be applicable to all candidates applying for a position at a Barings entity located within Singapore.

In the event of any conflict or inconsistency with the main body of the Job Applicant Privacy Notice, this Appendix H shall prevail.

Applicable Data Law

For the purposes of this Appendix H, Applicable Data Laws shall mean any applicable data protection laws relating to the protection of individuals with regard to the processing of personal data, including:

- (a) the Personal Data Protection Act 2012; and
- (b) any corresponding or equivalent national laws or regulations relating to the collection, use, disclosure and processing of personal data including any amendment, update, modification to or re-enactment of such laws and guides and codes of practice issued from time to time by any supervisory authorities, in each case as amended, updated or replaced from time to time.

Further, ("Personal Data") shall have the meaning ascribed to it in the Personal Data Protection Act 2012.

How Do I Access My Personal Data?

You may contact us in accordance with the Job Applicant Privacy Notice if you wish to find out about the Personal Data we hold about you or how we used or disclosed that Personal Data in the past 12 months prior to your request. We may need to verify your identity before giving you access and, depending on the complexity of your request, we may charge a reasonable fee for processing the request.

If we are unable to respond to your requests within thirty (30) days after receipt of your request, we will inform you within that time in writing the time by which we will be able to respond to the request.

How Do I Correct my Personal Data?

In order to ensure that the Personal Data that we maintain is accurate, you may, at any time, send our Data Protection Officer requests to update your information or requests for correction of errors or omissions in Personal Data which we hold about you.

If we are unable to respond to your requests within thirty (30) days after receipt of your request, we will inform you within that time in writing the time by which we will be able to respond to the request.

How Do I Withdraw my Consent?

You may withdraw consent and request us to stop using and/or disclosing your Personal Data for any or all of the purposes listed herein by submitting your request via email to our Data Protection Officer. We will inform you of the likely consequences of withdrawing consent and will endeavor to process your request within ten (10) business days from the day of receipt of your request.

Security

We will use technical and organisational measures to safeguard your Personal Data. For example: (a) all Personal Data you provide to us is stored on our secure servers; (b) we restrict access to Personal Data to our employees, service providers and contractors on a strictly need-to-know basis and ensure that those persons are subject to contractual confidentiality obligations; and (c) we review our Personal Data

collection, storage and processing practices from time to time to guard against unauthorised access, processing or use.

Retention of Personal Data

We will only retain and use your Personal Data for as long as the purpose for which that Personal Data was collected for is being served by retention of the Personal Data, or the retention is necessary for legal or business purposes, including complying with our legal obligations, resolving disputes and enforcing our agreements.

International Transfers

If we transfer any of your Personal Data to a country or territory outside Singapore, or to our group or affiliates companies located outside Singapore, or to a permitted third party located outside of Singapore, we will only do so if we ensure that the overseas receiving party is bound by legally enforceable obligations to afford the transferred data a standard of protection that is comparable to that under Singapore law. We will also ensure that any overseas recipient is able to provide appropriate technical and organisational measures to protect your Personal Data and its confidentiality.

Data Portability

To the extent applicable under the PDPA, as long as you have an existing direct contractual arrangement with us, you may send our Data Protection Officer a request for us to transmit your Personal Data, which was collected or created by us prior to the date of your request, which is in our possession or under our control, to another organisation in Singapore.

Complaints

If you believe that your privacy has been breached, please contact us in accordance with the Job Applicant Privacy Notice and provide details of the incident so that we can investigate and respond to you about your concerns.

We will review all communications and complaints submitted to us in this manner and will aim to respond to you in writing within a reasonable time. If your complaint is not satisfactorily resolved, you may submit a complaint to the Personal Data Protection Commission.

Data Protection Officer

Our Data Protection Officer can be contacted via email at DPM@Barings.com.

Barings Data Privacy Manager

20 Old Bailey, EC4MBF

London, UK

APPENDIX I - SWITZERLAND

This Appendix I shall be applicable to all candidates applying for a position at a Barings entity located within Switzerland.

In the event of any conflict or inconsistency with the main body of the Job Applicant Privacy Notice, this Appendix I shall prevail.

Applicable Data Law

For the purposes of this Appendix I, Applicable Data Laws shall mean any applicable data protection laws relating to the protection of individuals with regards to the processing of personal data, including:

- (c) **Article 328b of the Swiss Code of Obligations (“CO”);**
- (d) the Swiss Federal Act of Data Protection (“FADP”); and
- (e) any corresponding or equivalent national laws or regulations relating to the collection, use, disclosure and processing of personal data including any amendment, update, modification to or re-enactment of such laws and guides and codes of practice issued from time to time by any supervisory authorities, in each case as amended, updated or replaced from time to time.

International Transfers

Subject to Applicable Data Laws, transfers to other countries or jurisdictions may be permitted if the country or jurisdiction in question is in the European Economic Area (EEA), or recognised by the competent Swiss authorities to provide ‘adequate protection’ for personal data.

However, some transfers may be to countries or jurisdictions that are not considered to have adequate protection and, in that case, the Company shall use reasonable efforts to implement contractual safeguards and / or other measures as foreseen by Applicable Data Laws for the cross-border transfer of personal data, as required based on the legitimate transfer mechanism used.

We may transfer your personal data to the following countries: United Kingdom, European Union, United States, Hong Kong, Singapore, Japan, Korea, and Taiwan.

When you are in Switzerland, further information in relation to specific international transfers can be obtained by contacting Barings’ Data Privacy Manager at DPM@Barings.com.

Complaints

If you believe that your privacy has been breached, please contact us in accordance with the Job Applicant Privacy Notice and provide details of the incident so that we can investigate and respond to you about your concerns.

We will review all communications and complaints submitted to us in this manner and will aim to respond to you in writing within a reasonable time. If your complaint is not satisfactorily resolved, you may submit a complaint to the Swiss Federal Data Protection and Information Commissioner (“FDPIIC”).

Contact the Controller

To contact us in relation to the Job Applicant Privacy Notice, please use the following methods:

E-mail: DPM@Barings.com

Barings Data Privacy Manager

20 Old Bailey, EC4MBF

London, United Kingdom

Or

Baring Asset Management Switzerland Sàrl

rue du Marché 28

1204 Genève

APPENDIX J - TAIWAN

This Appendix J shall be applicable to all candidates applying for a position at a Barings entity located within Taiwan.

In the event of any conflict or inconsistency with the main body of the Job Applicant Privacy Notice, this Appendix J shall prevail.

Applicable Data Laws

For the purposes of this Appendix J, Applicable Data Laws shall mean any applicable data protection laws relating to the protection of individuals with regards to the processing of personal data, including:

- (a) the Taiwan Personal Data Protection Act;
- (b) the Enforcement Rules of the Personal Data Protection Act; and
- (c) any corresponding or equivalent national laws or regulations relating to the collection, use, disclosure and processing of personal data including any amendment, update, modification to or re-enactment of such laws and guides and codes of practice issued from time to time by any supervisory authorities, in each case as amended, updated or replaced from time to time.

International Transfers

Subject to the Applicable Data Laws, transfers to other countries or jurisdictions outside of Taiwan may be permitted except where the Taiwan National Communications Commission has issued an order to state that such transfer:

- (1) involves major national interests;
- (2) is prohibited under an international treaty or agreement;
- (3) is made to jurisdictions or countries providing inadequate protection for personal data [(including mainland China)] and may cause harm to the data subject's right; or
- (4) the cross-border transfer of the personal data to a third country is carried out to circumvent the Applicable Data Laws.

Special Category Data

Special Category Data shall, for purposes of this Appendix Q, include medical records, medical treatment, genetic information, sexual life (including sexual orientation) and health examination and criminal records.

In respect of any Special Category Data, you hereby consent to the personal information provided by you in the Form (including answers on gender, race/ethnicity, and whether you identify as a member of the LGBTQ+ community) may be processed for the purpose of carrying out diversity monitoring and activities if required by law and / or permitted by law, each in accordance with the Job Applicant Privacy Notice.

Your Additional Rights

You have rights, using the contact details below:

- to request copies of your Personal data; and
- to supplement your Personal data.

Contact Details

To contact us in relation to the Job Applicant Privacy Notice, please use the following methods:

E-mail: DPM@Barings.com

Barings Data Privacy Manager

20 Old Bailey, EC4MBF

London, United Kingdom

APPENDIX K – DIFC

This Appendix K shall be applicable to all candidates applying for a position at a Barings entity located within the Dubai International Financial Centre (“DIFC”).

In the event of any conflict or inconsistency with the main body of the Job Applicant Privacy Notice, this Appendix K shall prevail.

Applicable Data Laws

For the purposes of this Appendix K, Applicable Data Laws shall mean any applicable data protection and privacy laws of the DIFC relating to the protection of individuals with regards to the processing of personal data including the DIFC Law No. 5 of 2020 and the associated Data Protection Regulations 2020, including any amendment, update, modification to or reenactment of such laws and guides and codes of practice issued from time to time by any supervisory authorities, in each case as amended, updated or replaced from time to time.

Individual Rights in Relation to Personal Data

In addition to the rights set out at Paragraph F of the Job Applicant Privacy Notice, if your personal data is subject to Applicable Data Laws, you will also be entitled to not be discriminated against or adversely treated when exercising your personal data rights.

Direct Marketing

We currently do not use your personal data for marketing purposes.

International Transfers

Subject to the Applicable Data Laws, transfers to other countries or jurisdictions outside of the DIFC may be permitted where such transfer is made to jurisdictions or countries providing “adequate protection” for personal data, including to our related entities or third-party service providers in the following jurisdictions: United States, Hong Kong, Singapore, Japan, Korea, and Taiwan.

However, some transfers may be to countries or jurisdictions that do not have adequate protection and, in that case, the Company shall conduct the transfer in accordance with the transfer requirements set out in the Applicable Data Laws such as by putting in place “Standard Contractual Clauses” approved by the DIFC Commissioner of Data Protection and by adopting appropriate supplementary measures necessary to bring the level of protection of the personal data undergoing transfer up to a level of protection equivalent to that within the DIFC. You can request a copy of the measures applying to the transfer of personal data by using the contact information as stated below.

Complaints

If you believe that your privacy has been breached, please contact us using the details below and provide details of the incident so that we can investigate and respond to you about your concerns.

We will review all communications and complaints submitted to us in this manner and will aim to respond to you in writing within a reasonable time. Notwithstanding the above, you have the right to make a complaint at any time to the DIFC Commissioner of Data Protection, the DIFC supervisory authority, at commissioner@dp.difc.ae

Contact Us

To contact us in relation to the Job Applicant Privacy Notice, please use the following methods:

E-mail: DPM@Barings.com

Barings Data Privacy Manager

20 Old Bailey, EC4MBF

London, United Kingdom