

JOB APPLICANT PRIVACY NOTICE

WHAT IS THE PURPOSE OF THIS DOCUMENT?

InfraRed Capital Partners (US) LLC, InfraRed Partners LLP and Charles II Realisation LLP ("**InfraRed**") (together, "InfraRed") are, together, responsible for deciding how we hold and use personal information about you. You are being sent a copy of this privacy notice because you are applying for work with us (whether as an employee, worker, or contractor). It makes you aware of how and why your personal data will be used, namely for the purposes of the recruitment exercise, and how long it will usually be retained for. It provides you with certain information that must be provided under applicable data privacy laws, including the General Data Protection Regulation ((EU) 2016/679) (GDPR) and the California Consumer Privacy Act ("CCPA").

InfraRed is a "data controller" in relation to your personal data. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

Sun Life Assurance Company of Canada, Sun Life Financial Inc., Sun Life Global Investments Inc, Sun Life 2007-1 Financing Corp. Sun Life Assurance Company of Canada U.S Operations Holding Inc, Sun Life (U.S) HoldCo 2008, Inc and InfraRed (UK) Holdco 2020 Ltd (companies that are members of our group) are also data controllers in relation to your personal data. They are also required under data protection legislation to notify you of certain information in their own privacy notices. You can contact those controllers via InfraRed's DPO by emailing DPO@ircp.com for information about how to obtain a copy of those privacy notices. Should you be successful in your application to work with us, we will provide you with our staff privacy notice, which explains what additional personal information we hold about you during and after your working relationship with us, the basis on which we process it, with whom it is shared and how it is stored.

DATA PROTECTION PRINCIPLES

We will comply with data protection law and principles, which means that your data will be:

- Used lawfully, fairly and in a transparent way
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date
- Kept only as long as necessary for the purposes we have told you about
- Kept securely

THE KIND OF INFORMATION WE HOLD ABOUT YOU

In connection with your application for work with us, we will collect, store and use the following categories of personal information about you:

- The information you have provided to us in your curriculum vitae and covering letter
- Professional and employment-related information, such as your current or past job history or performance evaluations
- The information you have provided on your application, including name, telephone number, personal email address and compensation details

- Any information you provide to us during an interview and as part of the application process, including any information you voluntarily provide us about any medical conditions and/or disabilities
- Results from assessments
- Demographic information, such as your age, gender, and zip / post code
- Inferences drawn from the information that you have provided to us, as described above

Unless and until you are successful in your application to work with us, we will not ask you for any information about any medical conditions and/or disabilities you have. Should you voluntarily provide any such information to us, we will keep it secure and only use it for the purposes of providing appropriate adjustments at relevant stages of the application process.

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about candidates from the following sources:

- You, the candidate
- Recruitment suppliers, from which we collect the following categories of data: name, CV, current employer and relevant employment information. The processing of your data by a recruitment supplier is subject to the terms agreed between you and the relevant supplier.
- Publicly accessible sources such as LinkedIn

HOW WE WILL USE INFORMATION ABOUT YOU

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

- Assess your skills, qualifications, and suitability for the role
- Carry out background and reference checks, where applicable
- Communicate with you about the recruitment process
- Keep records related to our hiring processes
- Comply with legal or regulatory requirements

It is in our legitimate interests to decide whether to appoint you to a role since it would be beneficial to our business to appoint someone to that role.

We also need to process your personal information to decide whether to enter into a contract with you.

Having received your CV, covering letter, application form, any other relevant employment information, and if applicable, the results from any assessments, we will then process that information to decide whether you meet the basic requirements to be shortlisted for the role. If you do, we will decide whether your application is strong enough to invite you for an interview. If we decide to invite you for an interview, we will use the information you provide to us at the interview to decide whether to offer you the role. If we decide to offer you

the role, we will conduct pre-employment checks before confirming your appointment.

IF YOU FAIL TO PROVIDE PERSONAL INFORMATION

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully. For example, if we require a reference for this role, and you fail to provide us with relevant details, we will not be able to take your application further.

AUTOMATED DECISION-MAKING

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making. For some roles, we may ask a series of screening questions or for you to complete online assessments; the answers to those questions and the results of any assessments are reviewed by a member of our HR team before deciding whether to progress with an application.

DATA SHARING

Your personal information may be shared with other companies within our group where it is in our legitimate interests to do so for internal administrative purposes, as part of our recruitment activities. Access to your personal information is limited to those employees who need to know the personal information, including in our human resources and information technology departments.

We may be required transfer your personal data to Sun Life Assurance Company of Canada, Sun Life Financial Inc., Sun Life Global Investments Inc, Sun Life 2007-1 Financing Corp. Sun Life Assurance Company of Canada U.S Operations Holding Inc and Sun Life (U.S) HoldCo 2008, Inc, members of our group who operate outside the UK and the EEA [and some of which operate in the US, a territory which does not provide equivalent protection to your personal data to that which is available to you in the UK and the EEA, [your rights may be less easy to enforce, and may involve transfers of your personal data to the US intelligence services in certain situations]]. We have however used the Standard Contractual Clauses as a safeguard to facilitate this transfer.

Further details on the steps we take to protect your personal information in these cases, including in connection with transfers to the specific group companies we mention above, is available from us on request by contacting the HR department.

Why might you share my personal information with third parties?

We will only share your personal information with third parties for the purposes of processing your application, where required by law or where we have another legitimate interest in doing so (in particular, to respond to any claims, to protect our rights or the rights of a third party (including our employees)). We will share your personal information with the following categories of third parties:

- recruitment agencies, search firms and/ or head-hunters (defined as recruitment suppliers)
- cloud based service providers who provide us with our HR systems
- specialist suppliers of HR assessment tools and services
- information technology systems suppliers and support, including email archiving, back-up and disaster recovery and cyber security services

The cloud-based service providers from which we procure our HR systems, and our suppliers of HR

assessment tools will use, store and/or access your personal information from the United States of America (the U.S.). They and we have taken appropriate measures to ensure that your personal information is protected adequately when transferred to the U.S., by ensuring that the U.S. entities have signed up to the EU-US Privacy Shield (see further <https://www.privacyshield.gov/welcome>), or where they have not, by requiring them to enter into European Commission approved standard contractual arrangements.

All of those third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information

Save as expressly detailed above, we will never sell or rent any of your personal information to any third party without notifying you and/or obtaining your consent.

DATA SECURITY

We are committed to protecting personal information from loss, misuse, disclose, alteration, unauthorized access and destruction and take all reasonable precautions to safeguard the confidentiality of personal information. Although we make every effort to protect the personal information we hold about you, the transmission of information over the internet is not completely secure. As such, you acknowledge and accept that we cannot guarantee the security of your personal information transmitted to us over the internet and that any such transmission is at your own risk. Once we have received your personal information, we will use strict procedures and security features to prevent unauthorized access.

Where we have given you (or where you have chosen) a password which enables you to access any account with us, you are responsible for keeping the password confidential. We ask you not to share your password with anyone.

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

DATA RETENTION

How long will you use my information for?

We will retain personal information relating to unsuccessful applicants for a period of 12 months after receipt of your application for the relevant role. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal information in accordance with our data policies.

If you are successful in your application to work for us, we will retain your personal information for the period set out in our staff privacy notice.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your rights in connection with personal information

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

- Request access to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to

ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact DPO@ircp.com in writing.

We will consider all such requests and provide our response within a reasonable period (and in any event within one month of your request unless we tell you we are entitled to a longer period under applicable law). Please note, however, that these rights are not absolute and they will not apply in certain circumstances, or certain personal information may be exempt from such requests in certain circumstances, for example if we need to keep using the information to comply with our own legal obligations or to establish, exercise or defend legal claims.

If the rights don't apply, or an exception applies, we will tell you this when responding to your request. We may request you provide us with information necessary to confirm your identity before responding to any request you make.

RIGHT TO WITHDRAW CONSENT

If we rely on your consent for us to use your personal information in a particular way, but you later change your mind, you may withdraw your consent by contacting us at DPO@ircp.com and we will stop doing so.

DATA PROTECTION OFFICER

We have appointed a data protection officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority, or the relevant regulator in your country of residence, for data protection issues.

The practices described in this privacy policy statement are current as of September 2020.