

Personal Data Privacy Notice for Candidates

The purpose of this personal data privacy notice is to inform you about how your personal data is processed by Arcesium LLC and its subsidiaries including Arcesium UK LLP (“we”, “us”, “our”), when you apply for employment or an engagement with us. You must review and ensure you agree with what is described in this notice prior to submitting data to us.

This notice applies to all applicants worldwide. As privacy and data protection laws vary around the world and among the different United States, this notice may be required to be supplemented by certain jurisdiction-specific notices, disclosures, or authorizations. We identify that required supplementation throughout this notice, wherever it applies, and [here](#), in the last section of this notice. Although this notice may be translated into other languages for convenience, this English language version is the controlling version.

What information do we collect?

If you apply for employment or an engagement we may collect some or all of the following information about you:

- Your name, address, and contact details, including email address and telephone number;
- Your qualifications, skills, experience, and employment history;
- Sample work product such as examples of software code or your written work;
- Details about your current or expected future compensation / consultancy fee;
- Information about your nationality, residency, or entitlement to work in the relevant jurisdiction; and
- Any other information that you voluntarily provide to us.

If you apply via an online portal or similar means, we also may collect your IP address and, if you use a mobile device, your geolocation data.

Sometimes we will collect personal data about you from third parties. For example, we might:

- Obtain professional references from a former employer or other relevant reference that you identify to us;
- Conduct watchlist checks (to ensure candidates are not identified as restricted, sanctioned, or prohibited individuals and thus prohibited from certain activities or industries); and
- Engage a background check provider to undertake an employment, credit, and/or criminal background check.

Why do we process your personal data?

The provision of personal data by you is necessary in order for us to (a) fulfil our legal obligations (e.g., verify your eligibility to work in the applicable location), and (b) process your application and consider you for a position with us including by conducting interviews, collecting references, and undertaking certain types background checks all to make the most appropriate recruitment decisions for our business. Except as specifically identified below, **the lawful basis for our processing is compliance with our legal obligations and protecting our legitimate interests.**

Processing data from applicants allows us to:

- Review and manage candidate applications and supporting materials;
- Administer and manage offers and communications with candidates;
- Meet our obligations with respect to any recruiting agencies that are acting on your behalf; and
- Administer, manage, and improve our recruiting operations.

When we perform background checks related to credit history, we are required to provide applicants from certain jurisdictions with additional notices and disclosures and, in some cases, an opportunity to consent. If those requirements apply, you will receive links to those notices and disclosures, and a mechanism for providing or declining to provide such consent, at the email address you provided to us.

Similarly, when we perform background checks involving criminal record data (as in the case of roles that require a high degree of trust and integrity, and/or where we are required to undertake such checks to assist our clients in complying with their regulatory obligations), we are required to obtain the consent of, and provide special notices to, applicants from certain jurisdictions. If those requirements apply, you will receive links to those notices and a mechanism for providing or declining to provide such consent at the email address you provided to us.

Who has access to your personal data?

In connection with the purposes described above, we may disclose your personal data to:

- Our subsidiaries, service providers (e.g., providers of IT services and background check agencies), and advisors;
- Fraud prevention agencies and law enforcement agencies;
- Courts, governmental and non-governmental regulators, and ombudsmen;
- Any third party that acquires, or is interested in acquiring or securitizing, all or part of our assets, shares, partnership interests, and/or membership interests, or that succeeds us in carrying on all or a part of our businesses, whether by merger, acquisition, reorganization, or otherwise; or
- As required or permitted by law, including to comply with a subpoena or similar legal process or government request, or when we believe in good faith that disclosure is legally required or we have a legitimate interest in making a disclosure, such as where necessary to protect our rights and property.

We may disclose your personal data for the purposes described above to recipients (including our subsidiaries, service providers, and advisors) that are located in a country outside of the country from which it was originally collected, including India, the United Kingdom, and the United States. Not all countries have equivalent data protection laws. **You hereby expressly consent to the transfer of your personal data to recipients that are located outside your home jurisdiction, including the United States or India.** Under no circumstances do we sell personal data. In addition, unless you give us your explicit consent to do so, we will not use your personal data for any purposes unrelated to the purposes we describe in this notice.

For how long do we keep your data?

In accordance with our internal data retention procedures, we will retain your data for use in connection with prospective recruiting activities, including to source candidates for employment and engagement opportunities and to organize events with candidates.

The criteria that we use to determine retention periods include: (i) how long the personal data is needed for our prospective recruiting activities; (ii) the type of personal data collected; and (iii) whether we are subject to any legal, contractual or similar obligation to retain the data (e.g., mandatory data retention laws, government orders to preserve data relevant to an investigation, or data that must be retained for the purposes of litigation or disputes). If you do not agree to the use and retention of your personal data in this manner, or if you would like more information about applicable data retention policies, please contact us using the contact details provided below.

If your application for employment or an engagement is successful, your personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment/engagement. We will describe the retention periods that are associated with

personnel files in a new privacy notice that will be provided at the time of employment/engagement.

Updates to this notice

We periodically review and may modify this notice. If we make modifications, we will continue to uphold our commitment to keeping your personal data secure.

Enquiries, requests, or concerns

All inquiries, requests, or concerns regarding this privacy notice or relating to the processing of your personal data including all requests as detailed in the "IMPORTANT NOTICE OF CERTAIN ADDITIONAL RIGHTS" section below, should be sent to privacy@arcesium.com.

IMPORTANT NOTICE OF CERTAIN ADDITIONAL RIGHTS

In the European Economic Area ("EEA") and the United Kingdom ("UK"), the General Data Protection Regulation or "GDPR" will apply to the data processing we engage in for our recruiting activities when those activities occur in the context of our EEA and UK operations. More specifically, when you apply for a position that requires residency in the EEA or UK, or a position that, per its job description, will serve or support exclusively or primarily our EEA or UK business, you have the additional rights listed below. We further extend those rights to applicants we know to have been in the EEA or UK when they submitted their personal data.

All such applicants have a right to:

- Access – the right to obtain a confirmation that your personal data is being processed, receive access to your personal data (if we are in fact processing it), and other information about the processing of your personal data and a copy of the personal data we are processing.
- Rectification – the right to have your personal data corrected if it is inaccurate, and depending on the purposes of processing, you may also ask to have incomplete personal data completed.
- Erasure – also known as the "right to be forgotten," the right to request your personal data be deleted under certain circumstances such as if it is no longer needed for the original purpose it was collected for or if you withdrew your consent. The right of erasure does not apply under certain circumstances including if the processing is necessary for our compliance with a legal obligation.
- Restrict processing – the right to restrict processing of your personal data under certain circumstances such as if you contest the accuracy of the personal data (and only for so long as it takes to verify that accuracy), the processing is unlawful and you have requested restricting the processing rather than erasure, or if we no longer need the personal data but you need it to establish, exercise, or defend a legal claim.
- Portability – the right to receive the personal data you provided to us (and not any other information) under limited circumstances such as if the basis for processing the personal data was consent or necessary for the performance of a contract with you, or the processing is carried out by automated means.
- Automated processing – the right to not be subject to a decision based solely on automated processing, including profiling.

- Object to processing – the right to object to the processing of your personal data to the extent our basis for processing is our legitimate interests or in the performance of a task carried out in the public interest. If you object, we will stop processing your personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights, and freedoms or we require the personal data to establish, exercise, or defend a legal claim.

We will respond to your request to exercise any of the above rights in writing (including via email), or orally if requested, as soon as practicable and in any event not more than within one month after receipt of your request. In exceptional cases, we may extend this period by up to two months and we will tell you why. If you would like to exercise any of these rights, please contact us using the contact details provided above.

You have the right to complain to your data protection authority about our collection and use of your personal data. Please contact your local data protection authority for more information. Contact information for data protection authorities can be found [here](#).

Your Right to Withdraw Consent – As indicated [here](#), the lawful basis for our processing is compliance with our legal obligations and protecting our legitimate interests. The only exception to that rule is in connection with certain type of background checks as described [here](#) and [here](#). In those cases, or in any other case where we may indicate that the lawful basis on which we have collected and processed your personal data is your consent, you can withdraw your consent at any time by contacting us using the contact information above. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal data conducted in reliance on lawful processing grounds other than consent. For the avoidance of doubt, it is not a condition of any prospective contract with us that you agree to any request for consent to process personal data. If you fail to provide certain information when requested, however, please note that we may not be able to continue with your application or conclude any agreement with you or we may be prevented from complying with our legal obligations.