Privacy Notice – Job Applicant

What We Need

Our Personal Data Protection Policy governs the use and storage of your data.

Ryan ("Firm") is a Controller of the personal data you (data subject) provide us. We may collect the following types of personal data from you:

- Identity: name, home address, date of birth, age, place of birth, telephone numbers, email address, and SI/NI Number
- Details about personal life: reference and background checks, which include credit check and managed adjudication standard check, criminal convictions, details about litigation or claims pending or threatened, any ownership of intellectual property (i.e., copyrights, trademarks, URLs, or similar property), relatives employed by Firm and subsidiaries, and language proficiencies
- Professional details: employment history, education history, historic compensation, professional memberships, previous clients (including name and telephone number of the primary contact), details of major speaking engagements, professional licenses, copies of restrictive covenant agreements, tax experience, number of tax audits responsible for, management experience/expertise, periods of unemployment, reference details (employer, contact details, reasons for leaving, final salary, permission to contact them), certifications, qualifications, availability to work, and computer skills
- Economic, financial, and insurance data: current compensation package, bonus payments, salary history, largest annual gross fee amount that the data subject has generated directly
- Connection or traffic data: login ID, timestamp information, and IP address
- Sensitive Personal Data: the Firm may also process race, religion or belief, gender, and sexual orientation for diversity monitoring. The Firm may also identify whether an individual is legally authorized to work in the country

Why We Need It

We need your personal data to provide you with the following services:

- Management and administration of the recruitment process
- Background and other pre-employment checks

The Firm's legal basis for collecting this information includes:

- The legitimate business interests of the Firm
- Consent of the data subject

What We Do With It

Your personal data is obtained either directly from you or from a Firm-approved recruitment agency.

Hosting and storage of your data takes place in the following locations:

- Global HR system
- HR department in the U.K., U.S., and India
- The following vendors:
  1. Workday (HR Management System)
  2. HireRight (Background Check Provider)

We may disclose your data to certain vendors and other third parties to enable the Firm to do business, including:

- Background check providers
- Outside legal counsel

When the Firm transfers your personal data, it employs secure transfer methods such as TLS or other secure transfer protocols. Some information is transmitted by company e-mail under an appropriate confidentiality agreement with the recipient.

We seek to use reasonable organizational, technical, and administrative measures to protect personal data within the Firm. Unfortunately, no data storage or transmission system can be guaranteed to be 100% secure.

How Long We Keep It

Unless otherwise required by law, the Firm retains data on unsuccessful job applicants for one year following the hiring decision. If you are hired, the Firm will provide you with an Employee Privacy Notice, with information regarding retention of employee records contained therein.

What Are Your Rights?

You are entitled to receive information from the Firm regarding the Firm's treatment of your personal information.

You have the right to request rectification and/or erasure of personal data, or restriction of processing concerning your personal data, or to object to processing, as well as the right to data portability.

To exercise these rights, please contact us using the Firm’s Data Subject Access Request Form. You have been provided a copy of this form in connection with the application process.

If you still feel that your personal data has not been handled appropriately according to the law, you can contact the relevant data protection authority in your country (e.g., the Information Commissioner’s Office in the UK, the Privacy Commissioner in Australia, the National Authority for Data Protection in Hungary) and file a complaint with them.