

Privacy Policy Job applicant



Job applicant privacy policy

Introduction

This Data Privacy Notice covers practices for the Keesing Reference Systems B.V. Job applicant process including data collection, data processing and data sharing.

Data Collection

If you are interested to apply for a position at a Keesing Reference Systems B.V. or to learn more about a position you may be asked to provide personal information such as contact details or professional background qualification information. This could be collected from you by email, recruitment website(s) or by telephone. The information you provide will be processed and used by Keesing Reference Systems B.V. only for the job recruitment, applicant and placement process.

Global Operations, Country Data Transfers, Data Sharing

Keesing Reference Systems B.V. operate with recruiters for job positions. In the course of Keesing Reference Systems B.V. recruitment, personal data and professional information you provide to Keesing Reference Systems B.V. maybe processed, transferred, shared with individuals participating in the recruiting and interviewing process in Keesing Reference Systems. We may also use contracted third party suppliers or services in the job recruitment process. We also reserve the right to disclose your information as required by law, court order, or legal process served on us, when we believe that disclosure is necessary to protect our rights, or to combat suspected fraudulent activities.

Data Retention

We retain the information provided to us for a reasonable time period that allows for future job candidate recruitment, applicant and placement processing. Also we may retain some job candidate recruitment, applicant data that is necessary to comply with local legal and government reporting obligations.

Candidate Background Checks

Keesing Reference Systems B.V. may contract with trusted third parties to perform background check procedures on job candidates. However before a background check is performed we will contact you to obtain your permission for performance of a background check and to provide you with information about how you can obtain a copy of information from the background check third party supplier if you have questions or concerns.

Data Security

We have put in place reasonable administrative, technical, and physical safeguards to protect against unauthorized access to the information we collect. However, no security measures are 100% impenetrable and we cannot guarantee against all potential security breaches. Moreover, the transmission of information over the Internet is not inherently secure, and we are not responsible for the transmission of information over networks that we do not control. Your use of our website service demonstrates your assumption of these risks.

How We Secure Your Personal Information

We take commercially reasonable efforts to maintain security protections in accordance with industry best practices to protect data we collect from loss, alteration, destruction, misuse, and unauthorized access or disclosure.

To prevent unauthorized access, maintain data accuracy, and ensure the appropriate use of the personal information we collect, we have implemented physical, electronic, and administrative procedures. We utilize hashing, encryption, and de-identification techniques to help ensure your privacy is safeguarded.

We have policies to help maintain control and physical security of the facilities used to store data and only allow access to authorized personnel, restrict access to data to only those employees, contractors and agents that require it to provide and support our services. All our employees are bound by confidentiality obligations and may be subject to disciplinary or legal action if they fail to meet these responsibilities.

We process information in a way that is compatible with and relevant for the purpose for which it was collected. To the extent necessary for those purposes, we take reasonable steps to ensure that any information in our care is accurate, complete, current, and reliable for its intended use.

Subject Access Requests to Data Held

Some countries have Data Subject Access laws that provides you the right to access the personal data we hold about you. Should you wish to access the information held by us about you, please let us know by contacting us with your specific requests using the information in the Contact Us section below. If your personal details change, if you have any queries about how we use your information, or if you would like to modify or remove personal data about you that is being held by Us, then you should contact us with your specific requests using the information in the Contact Us section below.

Contact Us:

HR: hr@keesingtechnologies.com

Hogehilweg 17, 1101 CB Amsterdam, The Netherlands

Tel: +31 (0) 20 7157 806