



Candidate Vetting Privacy Policy

We will use the information you have given on your application form, together with any information that we obtain with your consent from third parties; for assessing your suitability for employment purposes only. It may be necessary to disclose your information to our agents and other service providers in order to carry out the background screening checks.

You will also be consenting to the transfer of your information to your current and future potential employers where this is necessary (this may be to companies operating abroad if you apply for work outside of the United Kingdom).

Your information will be held on our computer database and not be supplied to anyone other than your employer that is requesting the employment checks.

GDPR Statement

The General Data Protection Regulations (Regulation (EU) 2016/679) comes into force on 25 May 2018. Candidate Vetting (the Screening Company) has reviewed its' internal processes and procedures to ensure that we will meet GDPR regulations when introduced. All internal policies and procedures comply with the Regulations and we have implemented minor changes in respect of the personal data we process on behalf of applicants to ensure full compliance.

Candidate Vetting is registered with the UK Information Commissioner's Office (Registration Number: ZA269719). Candidate Vetting is fully committed to the principals of data protection and the protection of the privacy of individuals.

GDPR Privacy Notice

Who is collecting the data?

To execute our duties, it is necessary for Candidate Vetting to collect, store and process individuals' personal information. This includes information from and relating to clients, past employers, referees/personal references, other publicly available sources and individuals on whom we are asked to conduct background checks for employment purposes.

What data is being collected?

We hold personal data on individuals referred to us by the client. This consists of information which is necessary to conduct background checks for employment applications and avoid breaches of confidentiality such as name, address, data of birth, employment history, past salary provided by the applicants or obtained from other sources with their prior consent. We do not seek to collect Sensitive Personal Data. "Sensitive Personal Data" are personal data that reveal any racial or ethnic origin,



Candidate Vetting Privacy Policy

financial status, political opinion, philosophical belief, religion, trade-union membership, sexual orientation, or concerns health and sex life, genetic data, or biometric data.

What is the legal basis for processing the data?

Data shall be fairly and lawfully processed only with the applicants' knowledge and prior written consent of the individual concerned.

Candidate Vetting will collect and process appropriate personal data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements. We will not use the personal data for any reason other than that specified in the consent form. We do not sell or release personal information to third parties for marketing purposes. All reasonable technical and organisational measures shall be taken to prevent the misuse, loss/destruction or damage to personal data.

Will the data be shared with any third parties?

We will only share your personal information with prospective employers.

Candidate Vetting operates services worldwide. Some countries outside the European Economic Area may not have laws regulating the use and transfer of personal data; we will ensure that personal data is not transferred to these countries without suitable safeguards.

How will the information be used?

Candidate Vetting will not use the personal data for any reason other than that specified in the consent form for the purposes of conducting sufficient background screening checks for employment purposes. We do not sell or release personal information to third parties for marketing purposes.

How long will the data be stored for?

All data held by Candidate Vetting, which is processed data and/or personal/sensitive data is encrypted at rest and held in a secure personal cloud, which is ISO27001 Certified. All data is held and processed within the United Kingdom. Backup data is also held within our secure ISO27001-compliant personal cloud.

We retain data in accordance with current legislation and our Data Retention Policy. Data is retained for 7 years unless it is retained for an individual or organisation which has taken legal action. Once the operational or legal requirement to store the data has expired the personal information is destroyed in a secure manner. Any proposed future changes to the method or location at which data is stored will be reviewed in line with the requirements of GDPR legislation.



Candidate Vetting Privacy Policy

What rights does the data subject have?

All applicants have the right of access to their personal data through subject access requests and maintain the right to correct any inaccurate personal data. The Applicant also has the right in certain cases to have personal data erased as well as the right to move their personal data from one service provider to another.

How can the data subject raise a complaint?

Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.