Candidate Privacy Policy

Purpose

The purpose of this policy is to set out the Company's approach to the collecting and processing of personal data relating to job applicants during the recruitment process. The Company is committed to being transparent about how it collects and uses data and to meeting its data protection obligations.

This privacy policy details how the Company collects and uses personal information about you during and after the application process, in accordance with the General Data Protection Regulation (GDPR) and UK data protection laws. This notice may be amended or updated at any time.

This policy applies to all applicants regardless of your method of submitting your application, including via recruitment agencies and all other methods both internal and external to the Company.

Scope

What information does the Company collect?

The Company may collect a range of information about you, during the recruitment process, including:

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including benefit entitlements;
- whether or not you have a disability for which the Company needs to make reasonable adjustments during the recruitment process;
- information about your entitlement to work in the UK;
- assessment notes and scoring; and
- details of address and bank details if you are being reimbursed for travel to an interview.

The Company collects this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment including online tests.

Once a job offer has been made (and subsequently accepted by you) the Company will also collect personal data about you from third parties, such as references supplied by former employers and where applicable, information from criminal records checks. You will be fully informed during this process and consent obtained, where required.

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

Data Protection principles

Data Protection laws require the Company to ensure that personal data:

- is processed fairly and lawfully and transparently and, in particular, shall not be processed unless specific conditions are met;
- is collected for specified, explicit and legitimate purposes as set out in the Data Protection laws, and shall not be processed in any further manner incompatible with that purpose or those purposes;
- is adequate, relevant and limited to what is necessary in relation to those purpose(s);
- is accurate and, where necessary, kept up to date;
- is not be kept for longer than is necessary;
- is kept in a form which permits identification of the data subject for no longer than is necessary for the purpose(s);
- is processed in accordance with the rights of data subjects under the Data Protection laws; and
- is kept secure by the Company, taking appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal data.

Why does the Company process personal data?

The Company needs to process data to take steps at your request prior to entering into a contract with you. It also needs to process your data to enter into a contract with you.

In some cases, the Company needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

The Company has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the Company to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom an offer of employment will be made. The Company may also need to process data from job applicants to respond to and defend against legal claims.

Where the Company relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

The Company processes health information if it needs to make reasonable adjustments to the recruitment process for candidates who have a disability. This is to carry out its obligations and exercise specific rights in relation to employment.

For some roles, the Company is obliged to seek information about criminal convictions and offences. Where the Company seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment.

Who has access to data?

Your information will be shared internally for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the business area with a vacancy and IT staff if access to the data is necessary for the performance of their roles.

The Company will not share your data with third parties, unless your application for employment is successful and it makes you an offer of employment. The Company will then request references via a third party provider to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks.

How does the Company protect data?

The Company takes the security of your data seriously. It has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused, or disclosed, and is not accessed except by our employees in the proper performance of their duties. This includes internal procedures and standards to which our staff must adhere as well as physical and technical security measures such as the encryptions and user authorisations on our IT systems.

For how long does the Company keep data?

If your application is unsuccessful, the Company will confidentially destroy your information once 7 months has elapsed and providing the Company does not require the information as part of any legal proceedings. Where your data is required as part of legal proceedings, the data will be confidentially destroyed once legal proceedings are fully completed.

Data from internal applications (current employees) will be retained in line with the information contained in the Employee Privacy Policy. If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment. The periods for which your data will be held is contained within our Employee Privacy Policy.

If you have travelled over 100 miles to attend an interview, the Company will offer reimbursement of travel costs. Where you accept this offer, you will be asked to provide proof of bank details and address. This information will then be retained on file for 7 years in line with the statutory retention requirements for financial records

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the Company to change incorrect or incomplete data;
- require the Company to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the Company is relying on its legitimate interests as the legal ground for processing; and
- ask the Company to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the Company's legitimate grounds for processing data.

If you would like to exercise any of these rights, please contact Louise Rigden, louise.rigden@geberit.com or ashley.anderson@geberit.com. If you believe that the Company has not complied with your data protection rights, you can complain to the Information Commissioner.

Local Data Protection Co-ordinators:

Louise Rigden	louise.rigden@geberit.com
Ashley Anderson	ashley.anderson@geberit.com
Generic GDPR email address	gdpruk@geberit.com

Data Protection Officer for Geberit

Data Protection Officer	dataprotection@geberit.com

Registration details with the ICO

Geberit Sales Ltd	ZA349235
Geberit Service	ZA350860

If you believe that the Company has not complied with your data protection rights, you can complain to the Information Commissioner further details of which can be found at ico.org.uk.

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to the Company during the recruitment process. However, if you do not provide the information, the Company may not be able to process your application properly or at all.

You are under no obligation to provide information for equal opportunities monitoring purposes and there are no consequences for your application if you choose not to provide such information.

Automated decision-making

Recruitment processes are not based solely on automated decision-making.

Responsibilities

The Company's board of directors has overall responsibility for data protection compliance within the Company.

Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Head of Human Resources