

## Recruitment Privacy Notice

**Data Controller:** Whistl UK Ltd, Meridian House, Fieldhouse Lane, Marlow, Bucks SL7 1TB

**Key Contact:** Steve Betts, Director of Security, Audit & Compliance, SHE and CSR,  
Tel: 07795 358508 email: steve.betts@whistl.co.uk

As part of any recruitment process, Whistl collects and processes personal data relating to job applicants. Whistl is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

### What information does Whistl collect?

Whistl collects a range of information about you. This includes

- 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 Whistl needs to make reasonable adjustments during the recruitment process;
- information about your entitlement to work in the UK; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health, and religion or belief.

Whistl 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.

Whistl will also collect personal data about you from third parties, such as references supplied by former employers and information from criminal records checks. Whistl will seek information from third parties only once a job offer to you has been made and will inform you that it is doing so.

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

### Why does Whistl process personal data?

Whistl 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, Whistl 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.

Whistl 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 Whistl to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. Whistl may also need to process data from job applicants to respond to and defend against legal claims.

Whistl 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.

Where Whistl processes other special categories of data, such as information about ethnic origin, sexual orientation, health, religion or belief, age, gender or marital status, this is done for the purposes of equal opportunities monitoring with the explicit consent of job applicants, which can be withdrawn at any time.

For some roles, Whistl is obliged to seek information about criminal convictions and offences. Where Whistl 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.

If your application is unsuccessful, Whistl will keep your personal data on file in case there are future employment opportunities for which you may be suited. Whistl will ask for your consent before it keeps your data for this purpose and you are free to withdraw your consent at any time.

### **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.

Whistl will not share your data with third parties, unless your application for employment is successful and it makes you an offer of employment. Whistl will then share your data with former employers to obtain references for you, employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks.

Whistl will not transfer your data outside the European Economic Area.

### **How does Whistl protect data?**

Whistl takes the security of your data seriously. Whistl has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties. Where data is stored in electronic form access is restricted to authorised staff through password protected systems and backed up on a daily basis. Any paper based data is stored in secure locked filing systems. Full details of Whistl Data Protection Policy setting out how your data is protected can be found on Marvin.

Where Whistl engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

### **For how long does Whistl keep data?**

If your application for employment is unsuccessful, Whistl will hold your data on file for 6 months after the end of the relevant recruitment process. If you agree to allow Whistl to keep your personal data on file, Whistl will hold your data on file for a further 12 months for consideration for future employment opportunities. At the end of that period or once you withdraw your consent, your data is deleted or destroyed.

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 will be provided to you in a new privacy notice on appointment.

### **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 Whistl to change incorrect or incomplete data;
- require Whistl 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 Whistl is relying on its legitimate interests as the legal ground for processing; and
- ask Whistl to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override Whistl's legitimate grounds for processing data.

If you would like to exercise any of these rights, please contact a member of the HR team (hr@whistl.co.uk) or Steve Betts, Director of Security, Audit & Compliance, SHE and CSR (steve.betts@whistl.co.uk).

If you believe that Whistl has not complied with your data protection rights, you can complain to the Information Commissioner.

### **What if you do not provide personal data?**

You are under no statutory or contractual obligation to provide data to Whistl during the recruitment process. However, if you do not provide the information, Whistl 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.