Job Applicant Privacy Notice

POLICY

The Company is aware of its obligations under the General Data Protection Regulation (GDPR) and is committed to processing your data securely and transparently. This privacy notice sets out, in line with GDPR and data protection laws, the types of data that we collect and hold on you as a job applicant. It also sets out how we use that information, how long we keep it for and other relevant information about your data.

Data controller details

The Company is a data controller, meaning that it determines the processes to be used when using your personal data.

Data protection principles

In relation to your personal data, we will:

- process it fairly, lawfully and in a clear, transparent way
- collect your data only for reasons that we find proper for the course of your employment in ways that have been explained to you
- only use it in the way that we have told you about
- ensure / provide access to ensure it is correct and up to date
- keep your data for only as long as we need it or as is required by law to be retained
- process it in a way that ensures it will not be used for anything that you are not aware of or have consented to (as appropriate), lost or destroyed

Types of data we process

We hold many types of data about you, including:

- your personal details including your name, address, date of birth, email address, phone numbers
- your photograph
- gender
- marital status
- whether or not you have a disability
- information included on your CV including references, education history and employment history
- documentation relating to your right to work in the UK
- driving licence
- details of your criminal record.

How we collect your data

We collect data about you in a variety of ways including the information you would normally include in a CV or a job application cover letter, or notes made by our recruiting officers during a recruitment interview. Further information will be collected directly from you when you complete forms at the start of your employment, for example, your bank and emergency contact details. Other details may be collected directly from you in the form of official documentation such as your driving licence, passport or other right to work evidence.

In some cases, we will collect data about you from third parties, such as employment agencies, social media, former employers when gathering references or credit reference agencies.

Personal data is kept in personnel files or within the Company's HR and IT systems.

Why we process your data

The law on data protection allows us to process your data for certain reasons only:

- in order to perform the employment contract that we are party to
- in order to carry out legally required duties
- in order for us to carry out our legitimate interests
- to protect your interests and
- where something is done in the public interest.

All the processing carried out by us falls into one of the permitted reasons. Generally, we will rely on the first three reasons set out above to process your data.

We need to collect your data to ensure we are complying with legal requirements such as:

- carrying out checks in relation to your right to work in the UK and
- making reasonable adjustments for disabled employees.

We also collect data so that we can carry out activities which are in the legitimate interests of the Company. We have set these out below:

- making decisions about who to offer employment to
- making decisions about salary and other benefits
- assessing training needs
- dealing with legal claims made against us

If you are unsuccessful in obtaining employment, we may seek your consent to retain your data in case other suitable job vacancies arise in the Company for which we think you may wish to be considered. You are free to withhold your consent to this and there will be no consequences for withholding consent.

Special categories of data

Special categories of data are data relating to your:

- health
- sex life
- sexual orientation
- race
- ethnic origin
- political opinion
- religion
- trade union membership and
- genetic and biometric data.

We must process special categories of data in accordance with more stringent guidelines. Most commonly, we will process special categories of data when the following applies:

- you have given explicit consent to the processing
- we must process the data in order to carry out our legal obligations
- we must process data for reasons of substantial public interest
- you have already made the data public.

We will use your special category data:

- for the purposes of equal opportunities monitoring
- comply with the duty to make reasonable adjustments for disabled job applicants and with other disability discrimination obligations

We do not need your consent if we use special categories of personal data in order to carry out our legal obligations or exercise specific rights under employment law. However, we may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent and there will be no consequences where consent is withheld. Consent, once given, may be withdrawn at any time. There will be no consequences where consent is withdrawn.

Criminal conviction data

We will collect criminal conviction data only where it is appropriate given the nature of the role you are applying for and where the law permits us. Such data will usually be collected prior to your employment should you be successful in obtaining employment. We use criminal conviction data in order for us to carry out our legitimate interests and obligations to our clients and partners who require checks to be carried out in order for us to work on their projects.

We rely on the lawful basis of carrying out our legitimate interests to process this data.

If you do not provide your data to us

One of the reasons for processing your data is to allow us to carry out an effective recruitment process. Whilst you are under no obligation to provide us with your data, we may not able to process, or continue with your application if you do not.

Sharing your data

Your data will be shared with colleagues within the Company where it is necessary for them to undertake their duties regarding recruitment. This includes, for example, the HR department, those in the department who have responsibility for the vacancy for which you are applying for screening your application and interviewing you, the IT department in circumstances where you require access to our systems to undertake any assessments requiring IT equipment.

In some cases, we will collect data about you from third parties, such as employment agencies, and social media platforms.

If you are successful in your job application your data will be shared with third parties. We may share your data in order to:

- obtain references as part of the recruitment process;
- obtain a criminal records check; and
- make decisions about your fitness for work through our occupational health providers.

We do not share your data with bodies outside of the European Economic Area.

Protecting your data

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such. If you wish to obtain more information on our policies or processes, please contact the Data Protection Officer on dpo@ciphr.com.

Where we share your data with third parties, we will either have data sharing agreements in place or we will confirm that your data is being held securely and in line with GDPR requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

How long we keep your data for

In line with data protection principles, we only keep your data for as long as we need it for and this will depend on whether you are successful in obtaining employment with us.

If your application is not successful and we have not sought consent, or you have not provided consent upon our request to keep your data for the purpose of future suitable job vacancies, we will keep your data for 12 months once the recruitment exercise ends.

If we have sought your consent to keep your data on file for future job vacancies, and you have provided consent, we will keep your data for up to 18 months once the recruitment exercise ends. At the end of this period, we will delete or destroy your data, unless you have already withdrawn your consent to our processing of your data. Upon receipt of your withdrawal of consent, we will stop processing your information for the purposes you originally agreed to as soon as possible.

If your application is successful, your data will be kept and transferred to the systems we administer for employees. We have a separate privacy notice for employees, which will be provided to you.

Automated decision making

No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

Your rights in relation to your data

The law on data protection gives you certain rights in relation to the data we hold on you. These are:

- the right to be informed. This means that we must tell you how we use your data, and this is the purpose of this privacy notice
- the right of access. You have the right to access the data that we hold on you. To do so, you should make a subject access request and this should be put in writing to the Data Protection Officer on dpo@ciphr.com.
- the right for any inaccuracies to be corrected. If any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it
- the right to have information deleted. If you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it
- the right to restrict the processing of the data. For example, if you believe the data we hold is incorrect, we will stop processing the data (whilst still holding it) until we have ensured that the data is correct
- the right to portability. You may transfer the data that we hold on you for your own purposes

- the right to object to the inclusion of any information. You have the right to object to the way we use your data where we are using it for our legitimate interests
- the right to regulate any automated decision-making and profiling of personal data. You have a right not to be subject to automated decision making in way that adversely affects your legal rights.

Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use. There will be no consequences for withdrawing your consent. However, in some cases, we may continue to use the data where so permitted by having a legitimate reason for doing so.

If you wish to exercise any of the rights explained above, please contact the Data Protection Officer on dpo@ciphr.com.

Making a complaint

The supervisory authority in the UK for data protection matters is the Information Commissioner (ICO). If you think your data protection rights have been breached in any way by us, you are able to make a complaint to the ICO by contacting the helpline on 0303 123 1113.

Data Protection Officer

The Company's Data Protection Officer can be contacted on dpo@ciphr.com.