Job Applicant Privacy Notice

General Data Protection Regulation (GDPR)

March 2020

Human Resources

Public

V2.0

Job applicant privacy notice

Introduction

Embark Group (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, the types of data that we 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. This is a supplementary document to the Group Data Protection Policy, which is available upon request from the HR department.

This notice applies to external job applicants only.

Data controller details

The Company is a data controller, meaning that it determines the processes to be used when using your personal data. Our head office address is; Embark Group Limited, 7th Floor, 100 Cannon Street, London, EC4N 6EU. The Data Protection Officer for the Group is the Chief Risk Officer.

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 necessary for prospective employment
- only use it in the way that we have told you about
- ensure it is correct and up to date
- keep your data for only as long as we need it
- process it in a way that ensures it will not be lost, destroyed or used for anything that you are not aware of or have consented to (as appropriate)

How we collect your data

We may collect data about you in a variety of ways including the information you include in a CV, a job application covering letter/email, or notes made by our recruiting managers or HR during a recruitment interview. If you are successful during the recruitment process other information will be collected directly from you when you complete forms ahead of the start of your employment.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference, identity and criminal record check agencies.

Personal data is kept in both hard and soft copy files within the Company's HR and IT systems.

Types of data we process

We may hold many types of data about you, which may include:

- your personal details including your name, address, email address and phone numbers
- information included on your CV and pre-employment documentation including references, education, qualifications and employment history
- recruitment assessment documentation such as interview notes or test results
- documentation relating to your nationality and right to work in the UK which may include your photograph
- whether or not you have declared a disability.

Why we process your data

We have a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. Embark may also need to process data from job applicants to respond to and defend against legal claims. In some cases, we need to process data to ensure that we are complying with our legal obligations. For example, we are required to check a successful applicant's eligibility to work in the UK before employment starts.

Embark also 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.

If you are unsuccessful in obtaining employment, your data will not be used for any reason other than in the ways explained in relation to the specific application you have made. However, we may seek your consent to retain your data in case other suitable job vacancies arise in the Company which may be of potential interest to you. You are free to withhold your consent to this and there will be no consequences for withholding consent.

Special categories of data

There is certain data which falls within the subject of Special Category Data which includes data relating to your:

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

Data regarding health or medical conditions that is collected as part of the onboarding process may be processed for the following purposes:

- performing or exercising obligations or rights of you or the Company under employment law, such as not to discriminate against you or dismiss you unfairly, for example in order to establish whether any reasonable adjustments may need to be made to assist you in performing your duties.
- establishing, exercising or defending legal claims

Where we process other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that we use for these purposes is anonymised or is collected with your express consent, which can be withdrawn at any time. You are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

Criminal conviction data

As a regulated employer, we have an obligation to ensure the fitness and propriety of our employees in order to comply with our regulatory obligations. We therefore carry out criminal and financial record checks and this data will usually be collected as part of pre-employment screening, however, may also be collected during your employment.

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.

Sharing your data

Your data will be shared with colleagues within the Company where it is necessary for them to undertake their duties with regard to recruitment. This includes, for example, the HR department, hiring managers responsible for screening your application and interviewing you, the IT department 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, former employers when gathering references or credit reference, identity and criminal record check agencies.

In order to complete recruitment assessments, we may share your personal data with third parties, for the purposes of psychometric testing for example.

Your personal information is not shared with bodies outside of the European Economic Area prior to a job offer being made.

Once a job offer is made we will share your data with third parties that process data on our behalf in connection with payroll, benefits, learning and development, as well as for the administration of employee records. We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the European Economic Area (EEA). If we do, we take steps to ensure that your personal information is kept secure and processed to the same standards as we must uphold, in accordance with legal obligations and our GDPR Policy.

Protecting your data

The organisation takes the security of your data seriously. The organisation 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 the organisation engages third parties to process personal data on its behalf, they do so on the basis of written instructions, under a duty of confidentiality and with obligations to implement appropriate technical and organisational measures to ensure the security of 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 or not 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 six 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 12 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 in which case it will be deleted or destroyed upon your withdrawal of consent.

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 upon an offer of employment.

Automated decision making

No decision will be made about you 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. You can read more about this in our Group Data Protection Policy which is available upon request from our HR department
- **the right for any inaccuracies to be corrected.** If any data that we hold about you is incomplete or inaccurate, you can 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.

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 Group Data Protection Officer who is the Chief Risk Officer or to the ICO.