Privacy notice for online recruitment data

What is the purpose of this document?

Tilbury Douglas is committed to protecting the privacy and security of your personal information. This Privacy Notice describes how we collect and use personal information about you through our online recruitment system, in accordance with the General Data Protection Regulation (GDPR).

The Data Controller will be responsible for deciding how it holds and uses personal information about you. Tilbury Douglas is required under data protection legislation to notify you of the information contained in this Privacy Notice.

It is important that you read this Privacy Notice, together with any other Privacy Notice Tilbury Douglas may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

The kind of information we hold about you.

As part of all recruitment processes, Tilbury Douglas collects and processes personal data relating to job applicants and those registered for job alerts. We may even gain your contact details from publicly available information. We are committed to being transparent about how we collect and use that data and to meeting our data protection obligations.

We collect a range of information (including sensitive or special categories of personal information) about you when you visit this applicant tracking system. 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.
- details of your referees
- details of your job preferences for job alerts.
- whether or not you have a disability for which the organisation needs to make reasonable
- adjustments during the recruitment process.
- criminal records information.

- information about your entitlement to work in the UK; and
- equal opportunities monitoring information, including information about your gender, ethnic origin, age, sexual orientation, and religion or belief.

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

We will also collect personal data about you from third parties, such as references supplied by former employers or other third-party referees, information from criminal records checks (if applicable to your role) and information from occupational health checks. We will seek information from third parties only once a conditional job offer to you has been made and you have accepted the offer.

How we will use information about you

We need to process data to take steps at your request prior to entering into a contract with you. We also need to process your data to enter into a contract with you.

In some cases, we need to process data to ensure that we are complying with legal obligations (including requirements of applicable employment laws). For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

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. We may also need to process data from job applicants to respond to and defend against legal claims.

We process other special categories of data, such as information about ethnic origin, sexual orientation, age, health or religion or belief, for equal opportunities monitoring purposes.

We recognise that in some circumstances it would be in our legitimate interests for one of our recruitment team to add you to what we call our "Talent Pool" by registering your interest in a role on your behalf (or adding your details to our site if we have used a third party to search and select). Where the processing would involve collecting, handling or storing sensitive or special categories of personal data, and we do not have an alternative lawful basis to rely on, we will seek your consent to do this. You are not obliged to provide consent, and where consent has been issued, you will be entitled to withdraw it at any time.

Our recruitment processes do not rely on automated decision-making.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided, we do so in line with our data protection and recruitment of ex-offenders policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We do not envisage that we will hold information about criminal convictions as a matter of course.

However, from time to time and in certain circumstances, we may need to collect information about criminal convictions, but will only do so if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we would expect to collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We would use information about criminal convictions and offences in the following ways:

- DBS Checks (Safeguarding & Background Checking)
  On certain contracts we have a legal and/or commercial requirement to carry out criminal records background checks. Examples of this include but are not limited to working in regulated environments such as legal or financial services or for safeguarding in the provision of care or education. In such circumstances conviction data is managed within HR by a dedicated compliance team. Conviction data itself is not stored once validated and is securely destroyed. As per guidance on managing conviction data no certificate data is retained beyond a period of six months.
- DBS Checks (As part of government security vetting (BPSS) or as part of enhanced security clearance
- (CTC, SC or DV).
  For roles on certain contracts there is often a requirement to comply with formal Government vetting standards. As part of these checks a Basic Criminal Records Disclosure is required. As with routine criminal records checks, conviction data is managed within HR Compliance and convictions data is not stored beyond validation and is securely destroyed. As per guidance on managing conviction data no certificate data is retained beyond a period of six months.

Who has access to your 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, payroll, audit, IT staff in order to set up systems access and any other internal department deemed necessary for your employment purposes.

We will share your data with third parties during the application period if the role you are applying for requires online assessments.

We will then only share your data with other third parties if your application for employment is successful and we make you an offer of employment. We will then share your data with former employers to obtain references for you, employment background check providers to obtain necessary background checks, occupational health, and the Disclosure and Barring Service to obtain necessary criminal records checks.

As part of making an application for a role with Tilbury Douglas, you acknowledge that we have a legitimate interest in sharing your personal information with the third parties stated above or any others deemed necessary for your offer of employment to be finalised.

Transferring information outside the EU

We may transfer your personal data outside of the United Kingdom and the EEA solely for the purposes of corresponding with you in relation to the role/job alerts you have applied/registered for.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

How long will you use my information for?

If your application for employment is unsuccessful, we will hold your data on file for 12 months after the end of the relevant recruitment process in case there are future employment opportunities for which you may be suited (where you are added to our Talent Pool). We will notify you of your addition to the Talent Pool at the time of application and you are free to request the removal of your details from the Talent Pool at any time. At the end of that period (or if you make an earlier request to be removed), your data is archived and anonymised (your data will be unidentifiable so that it can still be used for reporting purposes), or any documents associated with you, deleted or destroyed. Interview notes for unsuccessful candidates will be held electronically by the interviewers and deleted/destroyed after 6 months.

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. Your personal data will then be subject to the terms of the Tilbury Douglas employee Privacy Notice (a copy of which will be made available to you upon commencing your employment).

Data Protection and Monitoring during employment- what you need to do.

You must comply with the Data Retention Disposal and the Data Protection policy when handling personal data during employment including personal data relating to any employee, worker, contractor, customer, client, supplier, or agent of the Company. Failure to comply with the Data Protection policies or any of the policies detailed in this agreement may be dealt with under the Company's disciplinary procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

The Company's systems enable the Company to monitor telephone, email, voicemail, internet, and other communications. In order to carry out its legal obligations as an employer (such as ensuring compliance with the Company's IT related policies), and for other business reasons, the Company may monitor use of systems including the telephone and computer systems, and any personal use of them, by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

Rights of access, correction, erasure, and restriction

Under certain circumstances, by law you have the right to:

- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

What happens to your data when you leave the Company?

In compliance with GDPR guidelines, statutory retention periods are recommended (up to 7 years dependant on various factors set by statute or standard practices) designed to protect former employees' privacy and to ensure that their personal data is kept only for as long as necessary. Once the retention period has expired, we will securely and permanently delete the data,

Below is a list of example documents and how long they should be kept for:

- Working time records – two years from the date to which they relate.
- Maternity, paternity, adoption, and shared parental leave pay records – three years after the end of the tax year in which the pay ceased. If an employee provides their child's birth certificate as evidence, then we will not keep a copy of this, only of the date of birth of the child.
- Income tax and National Insurance records – three years after the end of the tax year to which they relate.
- National Minimum Wage wage records – three years from the end of the pay reference period to which the record relates.
- Salary and pay generally – six years.
- Records of accidents in the workplace – at least three years since date the record was made.
- Application and recruitment records (including interview notes) – at least six months and up to twelve months for an unsuccessful candidate. If successful, these records will form part of the employee's personnel file.
- Parental leave records – five years from the birth or adoption, or until the child is aged 18 if they receive a disability allowance.
- Pensions benefits – six years, but only four years in relation to employees who opt out of the pension scheme.
- Disclosure and Barring Service (DBS) check – only for as long as is necessary and not usually for more than six months.
- Right to work documents – these should be kept for the duration of the person's employment and for two years after they have left.
- All personnel files and training records, including disciplinary, redundancy and sickness absence records – seven years from when the individual ceased to be employed by the Company.

Any further queries

If you have any questions about this Privacy Notice or how we handle your personal information, please contact td.recruitment@tilburydouglas.co.uk in the first instance so we can help you identify the appropriate Data Controller within Tilbury Douglas.

You have the right to make a complaint at any time to a national Data Protection Supervisory Authority. In the UK, this will be the Information Commissioner's Office (ICO), whose address is Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Telephone 0303 123 1113.