

## Privacy Notice – Job Applicants

### 1. What is the purpose of this document?

TWM Solicitors LLP and TWM Trust Corporation Ltd (jointly referred to herein as “TWM” and “We”) is a *Data Controller* and responsible for deciding how we hold and use *Personal Data* about you. You are being sent a copy of this privacy notice because you are applying for work with us (whether as an employee, worker or contractor). It tells you how and why your *Personal Data* will be used, namely for the purposes of the recruitment exercise, and how long it will usually be retained for. It provides you with certain information that must be provided under the Data Protection Act 2018 (DPA).

### 2. Definitions of terms in italics in this notice

***Automated Processing***: any form of automated *Processing of Personal Data* consisting of the use of *Personal Data* to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

***Consent***: agreement which must be freely given, specific, informed and be an unambiguous indication of the *Data Subject's* wishes by which they, by a statement or by a clear positive action, signifies agreement to the *Processing of Personal Data* relating to them.

***Data Subject***: a living, identified or identifiable individual about whom we hold *Personal Data*. *Data Subjects* may be nationals or residents of any country and may have legal rights regarding their *Personal Data*.

***Data Protection Officer (DPO)***: the person required to be appointed in specific circumstances under the *DPA*.

***Legitimate Interest***: the interest of the firm in conducting and managing its business to enable it to give clients the best service and the best and most secure experience. We make sure we consider and balance any potential impact on data subjects (both positive and negative) and their rights before we *Process* their personal data for our *Legitimate Interests*. We do not use their personal data for activities where our interests are overridden by the impact on them (unless we have their *Consent* or are otherwise required or permitted to by law).

***Personal Data***: any information identifying a *Data Subject* or information relating to a *Data Subject* that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. *Personal Data* includes *Sensitive Personal Data* and *Pseudonymised Personal Data* but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person’s actions or behaviour.

**Process or Processing:** any activity that involves the use of *Personal Data*. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. *Processing* also includes transmitting or transferring *Personal Data* to third parties.

**Sensitive Personal Data (now called Special Categories of Data in the DPA):** information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual orientation, biometric or genetic data, and *Personal Data* relating to criminal offences and convictions.

### 3. Data protection principles

TWM complies with data protection law and principles, which means that your data will 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.

### 4. Why we Process your Personal Data

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 *Personal Data* to enter into a contract with you.

In some cases, we need to *Process Personal Data* to ensure that it complies with our legal obligations. For example, we are 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 procedure and for keeping records of the *Process*. *Processing Personal 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 Personal Data* from job applicants to respond to and defend legal claims.

Where we rely on *Legitimate Interests* as a reason for *Processing Personal Data*, we have considered whether or not those interests are overridden by the rights and freedoms of candidates and have concluded that they are not.

### 5. The kind of information we hold about you

In connection with your application for work with us, we will collect, store, and use the following categories of *Personal Data* about you:

- (a) The information you have provided to us in your CV and covering letter;

- (b) If applying for a training contract, the information you have provided on our application form, including name, title, address, telephone number, personal email address, gender, employment history, qualifications including exam/degree/GDL/LPC details and results, positions of responsibility outside of employment, languages, charitable and pro bono endeavours, achievements, travel, other extra curricular activities, eligibility for employment in the UK, dates unavailable for interview and how you heard about TWM;
- (c) Any information you provide to us during an interview or prior to interview;
- (d) Test results, copies of relevant qualification certificates, your current practising certificate, your training record and a copy of your passport or other identification concerning your entitlement to work in the UK;
- (e) Information about your current level of remuneration, including benefit entitlements;
- (f) Information sought upon position being offered to you:
- Address;
  - telephone number;
  - and start date.
- (g) Information sought after the job offer has been accepted but prior to commencing employment:
- Criminal convictions and offences;
  - References;
  - Next of kin/emergency contact details;
  - Biography/profile for our intranet and a photograph;
  - Information for payroll purposes in the form of an HMRC Starter Checklist and/or P45 and a New Starter Form, including details such as bank account information, date of birth, NI number, student loan, PAYE number, tax code, earnings for the tax year, the amount you paid in tax in the tax year, and the date you finished working for your former employer;
  - Whether or not you have a disability for which TWM needs to make reasonable adjustments during the recruitment *Process*;
  - Equal opportunities monitoring information including socio economic background, caring responsibilities and “special category” information as mentioned below.
- (h) We may also collect, store and use the following *Special Categories of Sensitive Personal Data*:
- Information about your race or ethnicity, religion or belief, sexual orientation. Information about your health including any medical/health conditions, health and sickness records (information sought only after a job offer has been accepted but prior to commencing employment);

We will only collect and use *Sensitive Personal Data* (for example about your race or ethnicity, religious beliefs, sexual orientation and political opinions, trade union membership, health and sickness records) when we are entitled to do so, for example when that is with your explicit consent, or if you have manifestly made that information public, or if that is necessary for prescribed purposes laid down by law.

## 6. How is your *Personal Data* collected?

We collect *Personal Data* about candidates from the following sources:

- You, the candidate;
- Recruitment agencies;
- Job sites:

We collect the following categories of data from Recruitment Agencies and/or jobsites:

- (a) Name, title and gender;
  - (b) Your current location;
  - (c) Current level of remuneration details including benefit entitlements;
  - (d) Value of a following if appropriate and targets achieved;
  - (e) Employment history;
  - (f) Qualifications including exam/degree/GDL/LPC details and results;
  - (g) Positions of responsibility outside of employment, languages, charitable and pro bono endeavours, achievements, travel, extra curricular activities (if applicable);
  - (h) Whether you have a disability for which the organisation needs to make reasonable adjustments;
  - (i) Eligibility for employment in the UK; and
  - (j) Dates available for interview.
- The Solicitors Regulation Authority for background check purposes, from which we collect the following categories of data:
    - Fee earners: confirmation that you hold a current practising certificate, that you have been admitted to the roll of solicitors of England and Wales and that there are no findings or orders that have been made by the SRA and/or the Solicitors Disciplinary Tribunal against you;
    - Support Personnel: confirmation that you are not subject to any restrictions from the SRA limiting or prohibiting your right to work in a legal practice.
  - The Disclosure and Barring Service in respect of criminal convictions (collected via Atlantic Data software only after a job offer has been accepted but prior to commencing employment);

- Your named referees, from whom we seek to collect the following categories of data:
  - (a) Dates employed;
  - (b) Position(s) held;
  - (c) Professional and interpersonal skills including strengths and weaknesses;
  - (d) Number of days absent through sickness in the last year;
  - (e) Whether there was any form of formal performance management/disciplinary action within the last 12 months;
  - (f) Whether the referee would re-employ; and
  - (g) Any additional information the referee may wish to supply.

## **7. How we will use *Personal Data* about you**

We will use the *Personal Data* we collect about you to:

- Assess your skills, qualifications, and suitability for the work or role;
- Carry out background and reference checks, where applicable;
- Communicate with you about the recruitment Process;
- Keep records related to our hiring Processes; and
- Comply with legal or regulatory requirements.

It is in our *Legitimate Interests* to decide whether to appoint you to a role or provide certain work.

We also need to *Process* your *Personal Data* to decide whether to enter into a contract of employment or a contract for services with you.

Having received your CV and covering letter (and, in some cases, your application form), along with any additional information provided by a recruitment agency (see above) or provided directly to us by you (such as location and remuneration package), we will then review that information to decide whether you meet the basic requirements to be shortlisted for the role. If you do, we will decide whether your application is strong enough to invite you for an interview. If so, we will use the information you provide to us at the interview, and test results if applicable, to decide whether to offer you the role or work. If we decide to offer you the role or work, we will then take up references and carry out SRA and Law Society checks before confirming your appointment.

## **8. If you fail to provide *Personal Data***

If you fail to provide *Personal Data* when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to progress your application further.

## 9. How we use particularly Sensitive Personal Data

We will use your particularly *Sensitive Personal Data* in the following ways:

- We will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment *Process*, for example whether adjustments need to be made during a test or interview;
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual orientation to ensure meaningful equal opportunity monitoring and reporting.

## 10. Information about criminal convictions

Having regard to the nature of the firm's business and because it is in the *Legitimate Interests* of the firm and our clients that we do so, we will carry out a criminal records check, as detailed above, in relation to all successful job applicants prior to them commencing work at our offices.

We have in place a Data Privacy and Information Management Policy which details the safeguards we have in place in order to protect the privacy and legal rights of the subject of such criminal records checks.

## 11. Automated Processing / decision-making

You will not be subject to decisions that will have a significant impact on you based solely on *Automated Processing* decision-making.

## 12. Data sharing

We will share your *Personal Data* internally for the purposes of *Processing* your application. This includes members of the HR team, interviewers involved in the recruitment *Process*, managers in the business area with a vacancy and IT Personnel if access to the data is necessary for the performance of their roles. Prior to commencing employment your profile for our intranet and a photograph will be supplied to our Marketing team.

We will only share your *Personal Data* to third parties prior to commencement of employment as follows:

- Recruitment agencies when obtaining further information about you prior to and during the interview process, providing feedback following interview, offering you the role, dealing with issues prior to commencing employment and during any rebate periods;
- Atlantic Data to check criminal convictions (although this information is usually entered onto the software directly by you);
- The Solicitors Regulation Authority and the Law Society as detailed above; and
- Your named referees.

All of TWM's third party service providers are required to take appropriate security measures to protect your *Personal Data* in line with our policies and data protection legislation. We do not allow our third party service providers to use your personal data for their own purposes.

We only permit them to *Process* your *Personal Data* for specified purposes and in accordance with our instructions.

### **13. Data security**

We have put in place appropriate security measures to prevent your *Personal Data* from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your *Personal Data* to those employees, agents, contractors and other third parties who have a business need to know. They will only *Process* your *Personal Data* on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the HR Manager, Kathy Betts (contact details below).

Candidate *Personal Data* will be stored in a range of different places, in hard copy files, on the HR Portal and on other IT systems (including email).

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.

### **14. Data retention**

We will retain your *Personal Data* for a period of 6 months from receipt if it is an unsolicited job application (except for unsolicited agency CVs which are not retained) or 1 year from the date the vacancy is successfully filled if in response to a vacancy advertisement or briefing, and 18 months for shortlisted trainee applications. We retain your *Personal Data* for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your *Personal Data* in accordance with our data retention policy.

If we wish to retain your *Personal Data* on file, on the basis that a further opportunity may arise in future and we may wish to consider you for that, we will write to you separately, seeking your explicit *Consent* to retain your *Personal Data* for a fixed period on that basis.

### **15. Rights of access, correction, erasure, and restriction**

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

- Request access to your *Personal Data* (commonly known as a *Data Subject Access Request*). This enables you to receive a copy of the *Personal Data* we hold about you and to check that we are *Processing* it lawfully;
- Request correction of the *Personal Data* 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 Data*. This enables you to ask us to delete or remove *Personal Data* 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 Data* where you have exercised your right to object to *Processing* (see below);
- Object to *Processing* of your *Personal Data* 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 Data* for direct marketing purposes;

- Request the restriction of *Processing* of your *Personal Data*. This enables you to ask us to suspend the *Processing* of *Personal Data* about you, for example if you want us to establish its accuracy or the reason for *Processing* it;
- Request the transfer of your *Personal Data* to another party;

If you want to review, verify, correct or request erasure of your *Personal Data*, object to the *Processing* of your *Personal Data*, or request that we transfer a copy of your *Personal Data* to another party, please contact the HR Manager, Kathy Betts, by [email](#) or by writing to her at TWM Solicitors LLP, 65 Woodbridge Road, Guildford, Surrey GU1 4RD.

## 16. Right to withdraw *Consent*

When you apply for a role, you provide *Consent* for us to *Process* your *Personal Data* for the purposes of the recruitment exercise. We do not ask for such *Consent* if we do not need it. You have the right to withdraw your *Consent* for *Processing* for that purpose at any time. To withdraw your *Consent*, please contact the HR Manager. Once we have received notification that you have withdrawn your *Consent*, we will no longer *Process* your application and, subject to our retention policy, we will dispose of your personal data securely.

## 17. Person with overall responsibility for data protection at TWM

The person with ultimate responsibility for this Privacy Notice is the firm's Managing Partner, Compliance Officer for Legal Practice (COLP) and *Data Protection Officer*, Jamie Berry. He has overall responsibility for data protection, privacy and information management at TWM. If you have any questions about how we handle your *Personal Data*, email Jamie at [Jamie.berry@twmsolicitors.com](mailto:Jamie.berry@twmsolicitors.com) or by writing to him at TWM Solicitors LLP, 65 Woodbridge Road, Guildford, Surrey GU1 4RD.

Finally, you have the right to make a complaint at any time to the [ICO](#). We would, however, like the opportunity to deal with your concerns before you approach the ICO so please contact Jamie Berry as above in the first instance.

**Jamie Berry**  
**Managing Partner**  
**October 2023**