## \*\*[Company Name] Candidate Data Privacy Policy\*\*

\*\*Version:\*\* 1.0

\*\*Effective Date:\*\* [Date of Adoption]

\*\*Review Date:\*\* [Date, typically 1 year from Effective Date]

---

### 1. Purpose

This policy outlines [Company Name]'s commitment to protecting the personal data of candidates throughout the recruitment process, in accordance with the General Data Protection Regulation (GDPR) and applicable data protection laws. It ensures that candidate data is collected, processed, stored, and retained responsibly and ethically, respecting individual privacy rights.

### 2. Scope

This policy applies to all personal data collected from individuals applying for employment or other opportunities at [Company Name], regardless of their location. This includes data collected through online application portals, email, direct contact, recruitment agencies, or any other source. It applies to all employees, contractors, and third parties involved in the recruitment process on behalf of [Company Name].

### 3. Policy Statement

[Company Name] is committed to being a responsible data controller and processor of candidate personal data. We will:

\* \*\*Lawfulness, Fairness, and Transparency:\*\* Process candidate data lawfully, fairly, and in a transparent manner.

\* \*\*Purpose Limitation:\*\* Collect personal data for specified, explicit, and legitimate recruitment purposes only.

\* \*\*Data Minimisation:\*\* Collect only personal data that is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

\* \*\*Accuracy:\*\* Take reasonable steps to ensure that personal data is accurate and kept up to date.

\* \*\*Storage Limitation:\*\* Keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

\* \*\*Integrity and Confidentiality:\*\* Process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

\* \*\*Accountability:\*\* Uphold and demonstrate compliance with the principles of GDPR.

### 4. Definitions

\* \*\*Personal Data:\*\* Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

\* \*\*Processing:\*\* Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

\* \*\*Data Controller:\*\* The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. [Company Name] acts as the Data Controller for candidate data.

\* \*\*Data Processor:\*\* A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

\* \*\*Consent:\*\* Freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

### 5. Lawful Basis for Processing

[Company Name] will process candidate data based on one or more lawful bases, including:

\* \*\*Consent:\*\* Where the candidate has given explicit consent to the processing of their personal data for one or more specific purposes (e.g., to be considered for future roles).

\* \*\*Contractual Necessity:\*\* Where processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (e.g., processing information to offer employment).

\* \*\*Legal Obligation:\*\* Where processing is necessary for compliance with a legal obligation to which [Company Name] is subject (e.g., for employment verification).

\* \*\*Legitimate Interests:\*\* Where processing is necessary for the purposes of the legitimate interests pursued by [Company Name] or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. Legitimate interests will be carefully assessed and documented.

### 6. Candidate Data Collection and Processing

#### 6.1. Information Collected

We may collect the following types of personal data from candidates:

\* \*\*Contact Information:\*\* Name, address, email address, phone number.

\* \*\*Application Details:\*\* CV/Resume, cover letter, previous employment history, education, qualifications, skills.

\* \*\*Assessment Data:\*\* Results of skills tests, interview notes, psychometric assessments.

\* \*\*Right to Work Information:\*\* Passport details, visa status (where legally required for employment).

\* \*\*Diversity Monitoring Data:\*\* Information voluntarily provided regarding ethnicity, gender, disability (this will be anonymised or anonymised where possible for statistical purposes and will not be used in selection decisions).

\* \*\*References:\*\* Contact details of referees.

#### 6.2. Purposes of Processing

Candidate data is processed for the following legitimate purposes:

\* To assess suitability for a specific job vacancy.

\* To communicate with candidates regarding their application.

\* To conduct background checks and verify qualifications (where applicable and with consent).

\* To maintain a talent pool for future relevant opportunities (with explicit consent).

\* To ensure compliance with legal and regulatory obligations.

\* For anonymised statistical analysis to improve our recruitment processes.

#### 6.3. Consent Management

Where consent is the lawful basis for processing (e.g., for inclusion in a talent pool), [Company Name] will ensure that:

\* Consent is freely given, specific, informed, and unambiguous.

\* Candidates are informed of the purpose for which their data will be processed.

\* Candidates have the right to withdraw their consent at any time, and this will be clearly communicated.

### 7. Candidate Rights

Candidates have the following rights regarding their personal data:

\* \*\*Right to Access:\*\* To request access to their personal data and to receive a copy of it.

\* \*\*Right to Rectification:\*\* To request that inaccurate personal data be corrected.

\* \*\*Right to Erasure ('Right to be Forgotten'):\*\* To request the deletion of their personal data in certain circumstances.

\* \*\*Right to Restriction of Processing:\*\* To request that the processing of their personal data be restricted in certain circumstances.

\* \*\*Right to Data Portability:\*\* To receive their personal data in a structured, commonly used, and machine-readable format and to transmit that data to another controller.

\* \*\*Right to Object:\*\* To object to the processing of their personal data in certain circumstances.

\* \*\*Right to Withdraw Consent:\*\* To withdraw consent at any time if consent was the basis for processing.

\* \*\*Right to Lodge a Complaint:\*\* To lodge a complaint with a supervisory authority if they believe their data has been processed unlawfully.

Requests concerning these rights should be submitted to [Designated Department/Role, e.g., HR Department or Data Protection Officer]. [Company Name] will respond to such requests within one month, as required by GDPR.

### 8. Data Retention and Storage

Candidate personal data will be retained for no longer than is necessary for the purposes for which it was collected.

\* \*\*Unsuccessful Candidates:\*\* Data of unsuccessful candidates will be retained for a period of [Specify retention period, e.g., 6 months, 12 months] from the date of notification of the unsuccessful outcome. After this period, data will be securely deleted or anonymised. Candidates may be asked for consent to retain their data for longer periods for future opportunities.

\* \*\*Successful Candidates:\*\* Data of successful candidates will be transferred to their employee file and processed in accordance with the [Company Name] Employee Data Privacy Policy.

All candidate data will be stored securely, using appropriate technical and organisational measures to prevent unauthorised access, loss, or disclosure. Access to candidate data will be restricted to those employees who have a legitimate need to access it for recruitment purposes.

### 9. Third-Party Sharing and Data Processors

[Company Name] may engage third-party service providers (e.g., Applicant Tracking System providers, background check agencies) who may process candidate data on our behalf. In such cases, [Company Name] will ensure that:

\* A written data processing agreement (DPA) is in place with each processor, ensuring they meet GDPR requirements.

\* Processors provide sufficient guarantees of their compliance with GDPR.

\* Data is transferred securely and only to the extent necessary for the specified purpose.

### 10. Data Security

[Company Name] is committed to protecting candidate data from unauthorised access, disclosure, alteration, or destruction. This is achieved through:

\* Implementing appropriate technical and organisational security measures.

\* Regularly reviewing and updating security practices.

\* Providing training to employees on data protection and security.

\* Restricting access to candidate data to authorised personnel only.

### 11. Governance and Accountability

#### 11.1. Data Protection Officer (DPO)

[If a DPO is appointed, include:]

[Company Name] has appointed a Data Protection Officer (DPO) responsible for overseeing the implementation of this policy and ensuring compliance with data protection regulations. The DPO can be contacted at [DPO Contact Information].

#### 11.2. Training

All employees involved in the recruitment process will receive appropriate training on data protection principles, GDPR requirements, and this policy.

#### 11.3. Monitoring and Auditing

[Company Name] will regularly monitor and audit its recruitment processes to ensure ongoing compliance with this policy and GDPR.

### 12. Policy Review

This policy will be reviewed at least annually, or more frequently if there are changes to legislation, business practices, or risks, to ensure its continued effectiveness and compliance.

---

\*\*Approved by:\*\*

[Name and Title of Authorising Person]

\*\*Date:\*\* [Date of Approval]