## [Company Name] Data Protection Policy – Candidate Privacy

### 1. Purpose

This policy establishes the framework for the lawful and ethical processing of personal data pertaining to individuals applying for employment or other opportunities at [Company Name] (hereinafter referred to as "Candidates"). It aims to ensure compliance with the General Data Protection Regulation (GDPR) and other applicable data protection laws, fostering trust and transparency in our recruitment processes.

### 2. Scope

This policy applies to all personal data collected, processed, stored, and shared in relation to the recruitment and selection process for any role within [Company Name], regardless of the employment type or contract. This includes data collected through online application portals, direct submissions, recruitment agencies, and any other third-party sources involved in the recruitment process. This policy applies to all employees, contractors, and representatives of [Company Name] who are involved in the recruitment process and have access to Candidate data.

### 3. Policy Statement

[Company Name] is committed to protecting the privacy and personal data of all Candidates. We will process Candidate personal data solely for the legitimate purposes of recruitment and selection, ensuring that all processing activities are lawful, fair, transparent, and proportionate. We will implement appropriate technical and organizational measures to safeguard Candidate data against unauthorized access, loss, or disclosure.

### 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. For the purposes of this policy, [Company Name] is the Data Controller.

\* \*\*Data Subject:\*\* An identifiable natural person who is the subject of personal data. In this context, the Data Subject is the Candidate.

\* \*\*Third Party:\*\* A natural or legal person, public authority, agency or another body, other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

### 5. Lawful Basis for Processing

[Company Name] will process Candidate personal data on the following lawful bases, as applicable:

\* \*\*Consent:\*\* Where a Candidate has given clear consent to the processing of their personal data for one or more specific purposes (e.g., for future vacancies).

\* \*\*Performance of a Contract:\*\* Where processing is necessary for the performance of a contract with the data subject or to take steps at the request of the data subject prior to entering into a contract (e.g., processing data for an employment offer).

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

\* \*\*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. Our legitimate interests include assessing suitability for a role, managing the recruitment process efficiently, and ensuring a fair and equitable selection process.

### 6. Types of Personal Data Collected

The types of personal data collected during the recruitment process may include, but are not limited to:

\* \*\*Identification Data:\*\* Name, contact details (email address, phone number, postal address), date of birth.

\* \*\*Application Information:\*\* CV/Resume, cover letter, application form responses, details of previous employment and education, qualifications, skills, references.

\* \*\*Assessment Data:\*\* Results of interviews, psychometric tests, or other assessments.

\* \*\*Background Check Data:\*\* Information obtained through right-to-work checks, criminal record checks (where legally permissible and relevant to the role), or other background verification processes.

\* \*\*Diversity and Equal Opportunities Data:\*\* Voluntary demographic information (e.g., ethnicity, gender, disability status) collected solely for monitoring purposes and anonymised for reporting. This data will be processed with explicit consent and handled separately from the main application.

### 7. Data Collection and Usage

\* \*\*Collection:\*\* Personal data will be collected directly from Candidates via application forms, emails, and interviews. Data may also be collected from third parties, such as recruitment agencies or provided references, where explicitly permitted by the Candidate.

\* \*\*Usage:\*\* Candidate personal data will be used solely for the purposes of evaluating their suitability for the specific role applied for, conducting interviews, performing background checks (where applicable and consented to), and making employment decisions.

\* \*\*Retention:\*\* Candidate data will be retained for no longer than is necessary for the purposes for which the personal data is processed. For unsuccessful Candidates, data will be retained for a maximum of [Specify retention period, e.g., 12 months] from the date of the final decision. For successful Candidates, data will be transferred to their employee file. Candidates will be informed of the retention period at the point of data collection.

### 8. Candidate Rights

Candidates have the following rights regarding their personal data:

\* \*\*Right to be Informed:\*\* Candidates have the right to be informed about the collection and use of their personal data. This policy and specific privacy notices provided during the application process fulfill this requirement.

\* \*\*Right of Access:\*\* Candidates have the right to access their personal data and obtain confirmation that their data is being processed.

\* \*\*Right to Rectification:\*\* Candidates have the right to have inaccurate personal data rectified.

\* \*\*Right to Erasure (Right to be Forgotten):\*\* Candidates have the right to request the erasure of their personal data under certain circumstances.

\* \*\*Right to Restrict Processing:\*\* Candidates have the right to request the restriction of processing of their personal data under certain circumstances.

\* \*\*Right to Data Portability:\*\* Candidates have the right 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:\*\* Candidates have the right to object to the processing of their personal data under certain circumstances.

\* \*\*Rights in relation to Automated Decision Making and Profiling:\*\* Candidates have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects them.

Requests to exercise these rights should be submitted in writing to the Data Protection Officer. [Company Name] will respond to all valid requests within the timeframe stipulated by GDPR (typically one month).

### 9. Data Sharing and Disclosure

\* \*\*Internal Sharing:\*\* Candidate data will only be shared internally with those individuals involved in the recruitment and decision-making process who have a legitimate need to access it.

\* \*\*Third-Party Sharing:\*\* Candidate data may be shared with third parties such as recruitment agencies, background check providers, or assessment platforms, but only with the Candidate's explicit consent and where such sharing is necessary for the recruitment process. All third-party service providers are contractually obligated to protect Candidate data and process it only according to [Company Name]'s instructions.

\* \*\*International Transfers:\*\* Where Candidate data is transferred outside of the European Economic Area (EEA), [Company Name] will ensure that appropriate safeguards are in place to protect the data, such as Standard Contractual Clauses (SCCs) or other approved transfer mechanisms.

### 10. Data Security

[Company Name] implements appropriate technical and organizational measures to ensure the security of Candidate personal data, including:

\* \*\*Access Controls:\*\* Limiting access to Candidate data to authorized personnel only.

\* \*\*Encryption:\*\* Encrypting sensitive data where appropriate.

\* \*\*Secure Storage:\*\* Storing data in secure systems with robust security protocols.

\* \*\*Regular Audits:\*\* Conducting regular security audits and assessments.

\* \*\*Training:\*\* Providing data protection training to all personnel involved in the recruitment process.

### 11. Governance and Accountability

\* \*\*Data Protection Officer (DPO):\*\* [Company Name] has appointed a Data Protection Officer (DPO) responsible for overseeing data protection compliance. The DPO can be contacted at [DPO Email Address] or [DPO Phone Number].

\* \*\*Record Keeping:\*\* [Company Name] will maintain records of all processing activities related to Candidate data in accordance with GDPR requirements.

\* \*\*Data Protection Impact Assessments (DPIAs):\*\* DPIAs will be conducted for high-risk processing activities related to Candidate data.

\* \*\*Breach Notification:\*\* Any suspected or actual data breaches involving Candidate personal data will be handled in accordance with [Company Name]'s Data Breach Response Plan, including timely notification to the relevant supervisory authority and affected data subjects as required by GDPR.

### 12. Training and Awareness

All employees and contractors involved in the recruitment process will receive regular training on data protection principles, GDPR compliance, and this policy. Awareness campaigns will be conducted to reinforce the importance of protecting Candidate data.

### 13. Review and Amendment

This policy will be reviewed at least annually or as required by changes in legislation or business practices. Any amendments will be communicated to all relevant personnel and made available on the company intranet.

---

\*\*Policy Owner:\*\* [Department responsible for HR/Recruitment]

\*\*Date of Issue:\*\* [Date]

\*\*Version:\*\* [Version Number]