\*\*Company Name\*\*

\*\*Internal Policy: Personal Data Processing for Recruitment and Employment\*\*

\*\*Document Version:\*\* 1.0

\*\*Effective Date:\*\* [Insert Date]

\*\*Review Date:\*\* [Insert Date, typically 12 months from Effective Date]

\*\*Policy Owner:\*\* [Insert Department/Role, e.g., Head of Human Resources]

---

\*\*1. Purpose\*\*

The purpose of this policy is to ensure that Company Name (hereinafter referred to as "the Company") processes personal data of candidates and employees in a manner that is compliant with the General Data Protection Regulation (GDPR) and other applicable data protection laws. This policy outlines the principles, procedures, and responsibilities for the lawful, fair, and transparent processing of personal data throughout the recruitment and employment lifecycle.

---

\*\*2. Scope\*\*

This policy applies to all personal data collected, processed, stored, or otherwise handled by the Company in relation to:

\* Job applicants and candidates for employment, whether directly or indirectly sourced.

\* Employees of the Company.

\* Contractors and temporary workers engaged by the Company.

This policy governs all individuals within the Company who access, process, or are responsible for personal data related to recruitment and employment.

---

\*\*3. Policy Statement\*\*

The Company is committed to protecting the privacy and personal data rights of all individuals. We will process personal data in accordance with the GDPR principles, including:

\* \*\*Lawfulness, Fairness, and Transparency:\*\* Personal data will be processed lawfully, fairly, and in a transparent manner. Individuals will be informed about the processing of their data.

\* \*\*Purpose Limitation:\*\* Personal data will be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

\* \*\*Data Minimisation:\*\* Personal data collected will be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

\* \*\*Accuracy:\*\* Personal data will be accurate and, where necessary, kept up to date; inaccurate personal data will be rectified or erased without delay.

\* \*\*Storage Limitation:\*\* Personal data will be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

\* \*\*Integrity and Confidentiality:\*\* Personal data will be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

---

\*\*4. Lawful Basis for Processing\*\*

The Company will identify and document a lawful basis for all processing activities concerning personal data for recruitment and employment purposes. Common lawful bases include:

\* \*\*Consent:\*\* Explicit consent obtained from the individual for specific processing activities (e.g., retaining CVs for future opportunities).

\* \*\*Contractual Necessity:\*\* Processing is necessary for the performance of a contract with the individual or to take steps at the individual’s request prior to entering into a contract (e.g., processing data for employment contracts).

\* \*\*Legal Obligation:\*\* Processing is necessary for compliance with a legal obligation to which the Company is subject (e.g., payroll, tax, immigration checks).

\* \*\*Legitimate Interests:\*\* Processing is necessary for the purposes of the legitimate interests pursued by the Company 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 pursued by the Company may include recruitment, workforce management, and business operations, provided appropriate safeguards are in place and individual rights are respected.

---

\*\*5. Data Collection and Processing Practices\*\*

\*\*5.1. Recruitment Data:\*\*

\* \*\*Information Collected:\*\* Personal data collected during recruitment may include (but is not limited to) name, contact details, employment history, qualifications, skills, references, and any other information provided in applications, CVs, cover letters, or during interviews.

\* \*\*Purpose of Collection:\*\* To assess suitability for a specific role, manage the recruitment process, and communicate with candidates.

\* \*\*Transparency:\*\* Candidates will be provided with a clear Privacy Notice at the point of data collection, informing them about:

\* The types of data collected.

\* The purposes for processing.

\* The lawful basis for processing.

\* The recipients of the data.

\* Data retention periods.

\* Their rights as data subjects.

\* Contact details of the Data Protection Officer (DPO) or designated representative.

\* \*\*Data Minimisation:\*\* Only data relevant to the specific role and recruitment process will be collected.

\* \*\*Special Category Data:\*\* Any special category data (e.g., health information, ethnic origin) will only be collected where strictly necessary for a specific purpose (e.g., lawful employment quotas) and with explicit consent or another appropriate lawful basis.

\*\*5.2. Employee Data:\*\*

\* \*\*Information Collected:\*\* Personal data collected for employment purposes may include (but is not limited to) personal contact details, payroll information, bank details, performance records, training records, disciplinary information, and any other data required for employment administration and legal compliance.

\* \*\*Purpose of Collection:\*\* To manage the employment relationship, administer payroll and benefits, ensure compliance with employment law, manage performance, and facilitate employee development.

\* \*\*Transparency:\*\* Employees will be provided with a clear Privacy Notice upon commencement of employment, outlining the processing of their personal data.

\*\*5.3. Data Retention:\*\*

\* \*\*Candidates:\*\* Unsuccessful candidate data will be retained for a maximum of [Specify Retention Period, e.g., 6 months] following the conclusion of the recruitment process, unless explicit consent is obtained to retain it for future opportunities. Successful candidate data will be transferred to employee records.

\* \*\*Employees:\*\* Employee personal data will be retained for the duration of their employment and for a period thereafter as required by law or for legitimate business needs (e.g., pensions, references, tax records). Specific retention periods will be detailed in the Employee Privacy Notice and relevant retention schedules.

---

\*\*6. Candidate and Employee Rights\*\*

In accordance with GDPR, candidates and employees have the following rights concerning their personal data:

\* \*\*Right of Access:\*\* To request access to their personal data held by the Company.

\* \*\*Right to Rectification:\*\* To request correction of inaccurate personal data.

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

\* \*\*Right to Restriction of Processing:\*\* To request the limitation of the processing of their personal data.

\* \*\*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, where applicable.

\* \*\*Right to Object:\*\* To object to the processing of their personal data, particularly where processing is based on legitimate interests.

\* \*\*Rights Related to Automated Decision Making and Profiling:\*\* To not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

Requests to exercise these rights should be submitted in writing to [Specify Department/Email, e.g., hr@companyname.com]. The Company will respond to such requests within the statutory timeframe of one month.

---

\*\*7. Data Security\*\*

The Company will implement appropriate technical and organisational measures to protect personal data against unauthorised access, loss, destruction, or alteration. These measures include:

\* Access controls to systems containing personal data.

\* Secure storage of digital and physical records.

\* Regular security awareness training for all staff.

\* Use of encryption where appropriate.

\* Regular review and updating of security protocols.

---

\*\*8. Data Transfers\*\*

Personal data will not be transferred to countries outside the European Economic Area (EEA) unless adequate safeguards are in place to ensure the protection of personal data, in line with GDPR requirements. Such safeguards may include:

\* Adequacy decisions from the European Commission.

\* Standard Contractual Clauses (SCCs).

\* Binding Corporate Rules (BCRs).

---

\*\*9. Governance and Responsibilities\*\*

\* \*\*Data Protection Officer (DPO) / Designated Representative:\*\* [Insert Name/Role, e.g., The HR Director] is responsible for overseeing the implementation and adherence to this policy and for acting as the primary contact for data protection matters.

\* \*\*Human Resources Department:\*\* Responsible for the day-to-day processing of personal data for recruitment and employment, ensuring compliance with this policy and providing relevant privacy notices.

\* \*\*All Employees:\*\* All employees who handle personal data are responsible for adhering to this policy and for completing mandatory data protection training.

\* \*\*IT Department:\*\* Responsible for implementing and maintaining technical security measures to protect personal data.

---

\*\*10. Training and Awareness\*\*

All personnel involved in the processing of personal data for recruitment and employment will receive regular training on data protection principles, GDPR requirements, and the specifics of this policy.

---

\*\*11. Policy Review\*\*

This policy will be reviewed annually, or more frequently if there are material changes to legislation, Company practices, or data processing activities, to ensure its continued effectiveness and compliance.

---

\*\*12. Breach Notification\*\*

Any suspected or actual personal data breaches must be reported immediately to [Specify Department/Role, e.g., the DPO or Head of HR]. The Company has established procedures for responding to and reporting data breaches in accordance with GDPR requirements.

---

\*\*13. Related Documents\*\*

\* Company Privacy Notice (Candidates)

\* Company Privacy Notice (Employees)

\* Data Retention Schedule

\* Data Subject Request Procedure

---

\*\*Approval:\*\*

\*\*Approved By:\*\* [Name and Title of Authorised Signatory]

\*\*Signature:\*\* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\*\*Date:\*\* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_