# [Your Company Name] Data Protection Policy: Candidate Information

## 1. Purpose

This policy establishes the principles and procedures for the lawful and ethical processing of candidate personal data by [Your Company Name]. It ensures compliance with the General Data Protection Regulation (GDPR) and other applicable data protection laws, safeguarding the rights and freedoms of individuals whose data we process in the context of recruitment and selection.

## 2. Scope

This policy applies to all [Your Company Name] employees, contractors, and any third parties acting on behalf of [Your Company Name] who collect, store, process, transfer, or otherwise handle candidate personal data during the recruitment lifecycle. This includes data collected via our careers portal, email, job boards, recruitment agencies, interviews, and any other source.

## 3. Policy Statement

[Your Company Name] is committed to protecting the personal data of all candidates. We will process candidate information lawfully, fairly, and transparently, only for specified, explicit, and legitimate purposes. We will ensure that the data we collect is adequate, relevant, and limited to what is necessary for these purposes. Candidate personal data will be kept accurate and up-to-date, retained only for as long as necessary, and processed in a manner that ensures appropriate security.

## 4. Definitions

\* \*\*Candidate:\*\* Any individual who applies for a position or expresses interest in employment opportunities with [Your Company Name].

\* \*\*Personal Data:\*\* Any information relating to an identified or identifiable natural person (the data subject). This includes names, contact details, educational and professional history, qualifications, assessment results, and any other information provided during the application process.

\* \*\*Processing:\*\* Any operation performed on 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:\*\* [Your Company Name] as the entity determining the purposes and means of processing candidate personal data.

\* \*\*Data Subject:\*\* The identified or identifiable natural person to whom personal data relates (i.e., the candidate).

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

\* \*\*Special Categories of Personal Data:\*\* Information concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation.

## 5. Lawful Basis for Processing

[Your Company Name] will process candidate personal data based on one or more lawful bases as stipulated by Article 6 of the GDPR. The primary lawful bases for processing candidate data during recruitment are:

\* \*\*Consent:\*\* Where a candidate has given clear consent for their personal data to be processed for one or more specific purposes.

\* \*\*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., to provide a job offer).

\* \*\*Legal Obligation:\*\* Where processing is necessary for compliance with a legal obligation to which the controller is subject.

\* \*\*Legitimate Interests:\*\* Where processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. For recruitment, legitimate interests may include the need to assess a candidate's suitability for a role.

Where [Your Company Name] processes special categories of personal data (Article 9 GDPR), an additional condition for lawful processing must be met, such as:

\* \*\*Explicit Consent:\*\* Explicit consent of the data subject.

\* \*\*Employment Law:\*\* Processing is necessary for the purposes of carrying out the obligations and asserting the rights of the controller or the data subject in the field of employment and social security and social protection law.

## 6. Principles of Data Processing

[Your Company Name] will adhere to the following GDPR principles when processing candidate personal data:

\* \*\*Lawfulness, Fairness, and Transparency:\*\* Data will be processed lawfully, fairly, and in a transparent manner in relation to the data subject. Candidates will be informed about the data we collect, why we collect it, how we use it, and who we share it with.

\* \*\*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:\*\* Only personal data that is adequate, relevant, and necessary for the stated purposes will be collected.

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

\* \*\*Storage Limitation:\*\* Personal data will be kept in a form which 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 of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

## 7. Candidate Rights

Candidates have the following rights concerning their personal data:

\* \*\*Right to be informed:\*\* To be provided with clear and concise information about the processing of their data.

\* \*\*Right of access:\*\* To request a copy of their personal data held by [Your Company Name].

\* \*\*Right to rectification:\*\* To request correction of inaccurate or incomplete personal data.

\* \*\*Right to erasure (Right to be forgotten):\*\* To request the deletion of their personal data, subject to certain conditions and legal obligations.

\* \*\*Right to restrict processing:\*\* To request limitations on how their personal data is processed.

\* \*\*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 based on legitimate interests or for direct marketing purposes.

\* \*\*Rights in relation 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, unless certain exceptions apply.

Requests from candidates should be directed to the Data Protection Officer or the HR department. [Your Company Name] will respond to such requests within the timeframe stipulated by GDPR (generally one month).

## 8. Data Collection and Processing Practices

### 8.1. Data Collected

During the recruitment process, [Your Company Name] may collect the following categories of personal data:

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

\* \*\*Application Details:\*\* CV, resume, cover letter, job application form responses.

\* \*\*Educational and Professional History:\*\* Degrees, certifications, employment history, previous roles and responsibilities.

\* \*\*Skills and Qualifications:\*\* Technical skills, languages, soft skills.

\* \*\*Assessment Data:\*\* Results from tests, assessments, or interviews.

\* \*\*References:\*\* Contact details for professional references (provided by the candidate).

\* \*\*Equal Opportunity Monitoring Data:\*\* Information on gender, ethnicity, disability, etc. (collected voluntarily and anonymously for reporting purposes).

\* \*\*Right to Work Information:\*\* Documents to verify eligibility to work in the relevant jurisdiction.

\* \*\*Other Information:\*\* Any other relevant information provided by the candidate or obtained through background checks (with consent and legal justification).

### 8.2. Purpose of Processing

Candidate personal data is processed for the following purposes:

\* To assess suitability for a specific job vacancy.

\* To manage the recruitment and selection process.

\* To communicate with candidates regarding their application.

\* To comply with legal and regulatory obligations (e.g., right to work checks).

\* To maintain recruitment records for future opportunities (with explicit consent).

\* For anonymised statistical analysis and diversity monitoring.

### 8.3. Retention of Data

Candidate data will be retained in accordance with [Your Company Name]'s Data Retention Policy. Generally, unsuccessful candidate data will be kept for a maximum of [Specify Duration, e.g., 12 months] from the date of application or the conclusion of the recruitment process, unless the candidate has consented to longer retention for future opportunities. Successful candidate data will be transferred to their employee record and retained as per the employee data retention schedule.

### 8.4. Data Security

[Your Company Name] will implement appropriate technical and organisational measures to protect candidate personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage. This includes:

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

\* Utilising secure systems and databases.

\* Implementing encryption where appropriate.

\* Providing data protection training to relevant staff.

\* Conducting regular security assessments.

### 8.5. Data Sharing and Third Parties

Candidate personal data may be shared with:

\* \*\*Internal Departments:\*\* Hiring managers, HR personnel, and relevant decision-makers involved in the recruitment process.

\* \*\*Third-Party Service Providers:\*\* Recruitment agencies, background check providers, assessment platforms. These providers will be contractually bound to process data only on our instructions and to protect it appropriately.

\* \*\*Legal and Regulatory Authorities:\*\* Where required by law or for compliance purposes.

[Your Company Name] will ensure that any third-party recipients of candidate data are also compliant with GDPR and have appropriate data protection agreements in place. Data will not be transferred to countries outside the European Economic Area (EEA) unless adequate safeguards are in place to ensure a similar level of protection.

## 9. Governance and Accountability

### 9.1. Data Protection Officer (DPO)

[Your Company Name] has appointed a Data Protection Officer (DPO) who is responsible for overseeing data protection strategy and implementation, ensuring compliance with GDPR, and acting as a point of contact for data subjects and supervisory authorities.

\* \*\*Contact Information for DPO:\*\*

\* \*\*Name:\*\* [Name of DPO]

\* \*\*Email:\*\* [Email Address of DPO]

\* \*\*Phone:\*\* [Phone Number of DPO]

\* \*\*Address:\*\* [Address of DPO]

### 9.2. Responsibilities

\* \*\*HR Department:\*\* Responsible for the day-to-day management of candidate data, implementing this policy, and ensuring staff are trained.

\* \*\*Hiring Managers:\*\* Responsible for ensuring that candidate data is handled appropriately within their teams and that the principles of data minimisation and purpose limitation are adhered to during the interview process.

\* \*\*All Employees:\*\* Responsible for understanding and adhering to this policy and reporting any potential data breaches or concerns.

### 9.3. Training

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

## 10. Data Breach Response

In the event of a personal data breach concerning candidate information, [Your Company Name] will follow its Data Breach Response Plan, which includes:

\* Assessing the nature, scope, and impact of the breach.

\* Notifying the relevant supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

\* Notifying the affected candidate(s) without undue delay where the personal data breach is likely to result in a high risk to their rights and freedoms.

\* Taking appropriate measures to mitigate the effects of the breach and prevent future occurrences.

## 11. Policy Review

This policy will be reviewed at least annually, or more frequently if required by changes in legislation, guidance, or business practices.

## 12. Approval and Version Control

| Version | Date Approved | Approved By | Notes |

| :------ | :------------ | :----------------- | :---------------------------------- |

| 1.0 | [Date] | [Name/Title of Approver] | Initial Policy Creation |

| 1.1 | [Date] | [Name/Title of Approver] | [Summary of changes made] |