## [Company Name] Data Privacy Policy for Candidates

\*\*Version:\*\* 1.0

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

\*\*Last Reviewed:\*\* [Date]

---

### 1. Purpose

The purpose of this policy is to outline the principles and procedures governing the collection, processing, storage, and deletion of personal data of candidates applying for employment or other opportunities at [Company Name]. This policy 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.

### 2. Scope

This policy applies to all personal data collected from or about individuals who apply for positions at [Company Name], whether directly through our recruitment channels, via third-party recruiters, or through any other means. It covers all employees, contractors, and departments involved in the recruitment and selection process.

### 3. Policy Statement

[Company Name] is committed to protecting the privacy of its candidates and ensuring that all personal data collected and processed during the recruitment lifecycle is handled lawfully, fairly, and transparently. We will adhere to the principles of data minimization, purpose limitation, accuracy, storage limitation, integrity and confidentiality, and accountability as mandated by the GDPR.

### 4. Legal Basis for Processing

[Company Name] will only process candidate personal data where a lawful basis exists, which may include:

\* \*\*Consent:\*\* Where a candidate has explicitly given consent for their data to be processed for specific recruitment purposes.

\* \*\*Legitimate Interests:\*\* Where processing is necessary for the legitimate interests of [Company Name] or a third party, provided these interests are not overridden by the interests or fundamental rights and freedoms of the candidate. Examples include assessing suitability for a role, verifying qualifications, and ensuring fair recruitment practices.

\* \*\*Contractual Necessity:\*\* Where processing is necessary for the performance of a contract or to take steps at the request of the candidate prior to entering into a contract (e.g., for background checks required for a job offer).

\* \*\*Legal Obligation:\*\* Where processing is necessary for compliance with a legal obligation to which [Company Name] is subject.

### 5. Types of Personal Data Collected

We will only collect personal data that is relevant and necessary for the recruitment process. This may include, but is not limited to:

\* Contact information (name, address, email, phone number)

\* Application details (CV, cover letter, resume)

\* Employment history and qualifications

\* Educational background

\* Skills and experience

\* References

\* Information related to diversity and inclusion (collected voluntarily and anonymized for reporting purposes where applicable)

\* Information obtained through background checks and eligibility to work verification

### 6. Collection and Use of Personal Data

\* \*\*Lawfulness, Fairness, and Transparency:\*\* Candidates will be informed about the collection and use of their personal data, including the purpose of processing, the types of data collected, the legal basis for processing, and their rights. This information will typically be provided via a privacy notice at the point of data collection.

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

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

\* \*\*Accuracy:\*\* We will take reasonable steps to ensure that personal data is accurate and kept up to date. Candidates are encouraged to inform us of any changes to their personal details.

\* \*\*Storage Limitation:\*\* Personal data will be retained for no longer than is necessary for the purposes for which it was collected. Our data retention policy for candidate data is detailed in Section 9.

\* \*\*Integrity and Confidentiality:\*\* Appropriate technical and organizational measures will be implemented to protect personal data against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

### 7. Candidate Rights

Candidates have the following rights under the GDPR regarding their personal data held by [Company Name]:

\* \*\*Right to be Informed:\*\* The right to be informed about the collection and use of their personal data.

\* \*\*Right of Access:\*\* The right to access their personal data and supplementary information.

\* \*\*Right to Rectification:\*\* The right to have inaccurate personal data rectified or completed if it is incomplete.

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

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

\* \*\*Right to Data Portability:\*\* The right to receive personal data in a structured, commonly used, and machine-readable format and to transmit that data to another controller under certain circumstances.

\* \*\*Right to Object:\*\* The right to object to the processing of their personal data under certain circumstances.

\* \*\*Rights in Relation to Automated Decision Making and Profiling:\*\* 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 regarding these rights should be submitted in writing to the Data Protection Officer or the designated HR contact. We will respond to all valid requests within the timeframe stipulated by the GDPR.

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

[Company Name] may share candidate personal data with third-party service providers who assist us in the recruitment process (e.g., Applicant Tracking Systems, background check providers). These third parties are contractually obligated to process data only on our instructions and to implement appropriate security measures. We will ensure that any such sharing complies with GDPR requirements, including having appropriate data processing agreements in place. Personal data will not be shared with third parties for marketing purposes without explicit consent.

### 9. Data Retention and Deletion

\* \*\*Unsuccessful Candidates:\*\* Personal data of unsuccessful candidates will be retained for a maximum of [Specify Time Period, e.g., 12 months] from the date of the final decision on their application. After this period, data will be securely deleted unless the candidate has provided explicit consent for their data to be retained for future opportunities.

\* \*\*Successful Candidates:\*\* Personal data of successful candidates will be transferred to their employee file and retained in accordance with the company's employee data retention policy.

\* \*\*Data Deletion Procedures:\*\* Secure deletion methods will be employed to ensure that data is irretrievably removed.

### 10. Data Security

[Company Name] will implement and maintain appropriate technical and organizational security measures to protect candidate personal data against loss, misuse, unauthorized access, disclosure, alteration, and destruction. These measures include, but are not limited to, access controls, encryption, regular security assessments, and employee training.

### 11. Governance and Accountability

\* \*\*Data Protection Officer (DPO):\*\* The designated Data Protection Officer (or equivalent role) is responsible for overseeing the implementation and enforcement of this policy and for ensuring compliance with GDPR.

\* \*\*Training:\*\* All employees involved in the recruitment process will receive regular training on data protection principles and this policy.

\* \*\*Monitoring and Auditing:\*\* [Company Name] will regularly monitor and audit its recruitment processes to ensure ongoing compliance with this policy and data protection regulations.

\* \*\*Breach Notification:\*\* Any suspected or actual personal data breaches will be handled in accordance with the company's data breach response plan and reported to the relevant supervisory authority and affected individuals where required by law.

### 12. Policy Review

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

---

\*\*Approved by:\*\*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Name and Title of Authorizing Authority]

[Date]