LEGAL & PRIVACY

Candidate Privacy Policy & Terms of Use

Version 1.0 · Effective 5 June 2026 · Next review 5 June 2027

CONTENTS

1. Introduction

This Privacy Policy and Terms of Use (**"Policy"**) describes how Lightico (**"Company"**, **"we"**, **"us"**, or **"our"**) collects, processes, stores, and protects personal data submitted through our AI-powered Applicant Tracking System (**"ATS"** or **"Platform"**). It applies to all job candidates (**"you"**, **"Data Subject"**) who interact with the Platform.

By submitting your information through the Platform, you acknowledge that you have read and understood this Policy. If you do not agree, please do not submit your personal data.

This document applies to Lightico Ltd and Vizolution Ltd trading as Lightico.

2. Data Controller

Lightico acts as the Data Controller for personal data collected through the Platform, as defined under GDPR Article 4(7) and equivalent legislation.

Contact details of the Data Controller:

- **Company:** Vizolution Ltd
- **Address:** Bay Studios, Swansea, United Kingdom, SA1 8QB
- **Privacy enquiries:** privacy@lightico.com

- **Data Protection Officer:** dataprotectionofficer@lightico.com

3. Personal Data We Collect

We collect only the personal data necessary for the recruitment process (data minimisation principle, GDPR Art. 5(1)(c)):

Data Type	Purpose / Legal Basis
Full name & contact details	Identifying the candidate and enabling communication — Legitimate interest / Pre-contractual steps (GDPR Art. 6(1)(b)(f))
CV / Resume content	Evaluating professional qualifications — Consent (GDPR Art. 6(1)(a)) or pre-contractual steps
Application metadata	Timestamping and audit trail — Legitimate interest
Usage data (logs, IP address)	Security, fraud prevention, system integrity — Legitimate interest

> **Special-category data:** We do NOT actively collect data such as race, religion, health, or biometric information (GDPR Art. 9 / Israeli PPL). CVs may incidentally contain such information; it is processed only to the extent necessary to evaluate the application, and our AI system does not highlight or summarise special-category data.

4. Use of Artificial Intelligence (AI)

Our HR professionals use AI to assist the recruitment process. We are transparent about the following:

4.1 How AI is Used

- AI assists HR users in reviewing, organising, and surfacing relevant candidate information.
- AI may generate summaries, highlights, or recommendations based on your CV and application data.
- **AI does NOT make autonomous hiring decisions.** Every consequential decision (advancing a candidate, rejection, offer) requires human review and approval.

4.2 Data Sent to AI Services

To power AI features, anonymised or pseudonymised portions of application data may be processed by a third-party AI provider. We implement the following safeguards:

- Personally Identifiable Information (PII) — such as name, email, and phone number — is stripped before data is sent to the AI model.
- We use Claude (Anthropic) for AI processing under a Data Processing Agreement (DPA) that prohibits use of data for model training.
- Data transmitted to the AI is subject to Anthropic's data privacy commitments.

4.3 Your Rights Regarding Automated Processing

Under GDPR Article 22, you have the right not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects. Since human review is always part of our process, Art. 22 restrictions are not triggered. Nonetheless, you may request a

manual review of any AI-generated assessment by contacting us at privacy@lightico.com.

4.4 EU AI Act Compliance (High-Risk Classification) From August 2026

Our Platform is classified as a high-risk AI system under EU AI Act Annex III, Category 4. As the deployer, we comply with the following obligations:

- **Human oversight:** every AI-generated output is labelled "AI-assisted". HR users must explicitly confirm they have reviewed the full CV before advancing or rejecting a candidate.
- **Transparency:** candidates are informed that AI is used in the recruitment process (this Policy, Section 4.1).
- **Bias monitoring:** quarterly reviews of AI output patterns to detect and remediate any discriminatory trends.
- **Logging:** all AI-generated outputs are logged with a pseudonymised candidate ID, timestamp, and HR user identifier for audit purposes.
- **No sole automation:** AI output cannot serve as the sole basis for any hiring decision — enforced at the application level.
- **Conformity assessment:** we maintain a documented EU AI Act Conformity Assessment available to supervisory authorities upon request.

4.5 Data Protection Impact Assessment (DPIA)

Processing personal data using AI in a recruitment context constitutes high-risk processing under GDPR Article 35. We have conducted a DPIA prior to going live, covering the nature and purpose of processing, necessity and proportionality, identified risks, and mitigating measures. A summary is available upon written request to dataprotectionofficer@lightico.com.

5. Legal Bases for Processing

We rely on the following legal bases, depending on the context:

- **Consent (GDPR Art. 6(1)(a))** — when you voluntarily submit your CV and application.
- **Pre-contractual steps (GDPR Art. 6(1)(b))** — to assess your suitability for a position.
- **Legitimate interests (GDPR Art. 6(1)(f))** — for system security, fraud prevention, and platform improvement, balanced against your rights.
- **Legal obligation (GDPR Art. 6(1)(c))** — where required by Israeli or other applicable law.

5.1 Records of Processing Activities (RoPA) — GDPR Art. 30

We maintain an internal Record of Processing Activities (RoPA) documenting all personal data processing operations. It is not publicly available but is accessible to supervisory authorities upon request. Candidates may request a summary of relevant RoPA entries by contacting dataprotectionofficer@lightico.com.

6. Data Sharing & Third Parties

We share personal data only as described below and **never sell your data**.

6.1 Cloud Infrastructure

Your data is stored on cloud infrastructure (AWS, GCP, or Azure). These providers act as Data Processors under signed DPAs and are certified under ISO 27001 / SOC 2. Where data is

transferred outside the EEA, we rely on EU Standard Contractual Clauses (SCCs) or equivalent mechanisms.

6.2 AI Processing (Anthropic)

As noted in Section 4, anonymised data may be processed by Anthropic's Claude API solely for AI feature delivery. No PII is transmitted.

6.3 Hiring Companies

If you apply for a position at a client company using our Platform, your application data will be shared with that company. They become an independent Data Controller for their recruitment process and are subject to their own privacy policy.

6.4 Legal Requirements

We may disclose data to law enforcement or regulatory bodies where required by applicable law, a court order, or to protect legal rights.

7. International Data Transfers

Your data may be transferred and processed outside your country of residence. We ensure adequate protection through:

- EU Standard Contractual Clauses (SCCs) — for transfers from EEA countries.
- Adequacy decisions — where applicable (e.g. Israel has an EU adequacy decision).
- Data Processing Agreements — with all sub-processors.
- Compliance with Israeli Privacy Protection Regulations 5784-2023 regarding cross-border transfers.
- Israeli database registration: our platform holds fewer than 1,000 candidate records and does not currently meet the threshold for mandatory registration. We maintain registration-ready documentation and will register with the Privacy Protection Authority (PPA) if and when the threshold is reached.

8. Data Retention & Deletion

8.1 Retention Periods

Data Type	Retention Period
CV / Resume & application data	Duration of recruitment process + up to 24 months after closure (with consent). Deleted upon your request or at end of retention period.
Contact details (name, email, phone)	Same as CV — linked to the application lifecycle.
AI-generated summaries / assessments	Deleted together with the associated application record.
Audit logs & system logs	Up to 7 years where required by applicable law.
Anonymised / aggregated statistics	May be retained indefinitely — they contain no personal data.

8.2 How to Request Deletion

You have the right to request deletion of your personal data at any time (GDPR Art. 17; Israeli Privacy Protection Law; CCPA):

- Email privacy@lightico.com with subject line: *Data Deletion Request*.
- Include your full name and the email address used when applying.
- We will confirm receipt within 5 business days and complete deletion within 30 days (GDPR) / 45 days (CCPA).

8.3 What Gets Deleted

Upon a confirmed deletion request, we will permanently erase your CV and uploaded documents, contact details, application form responses, AI-generated summaries, and candidate account credentials.

8.4 What May Be Retained After Deletion

Certain data may be legally exempt from deletion: audit logs and anonymised records required by law (retained up to 7 years with no personal identifiers); data subject to an active legal dispute or court order; and aggregated, non-identifiable statistics. We will inform you of any retained data and its legal basis within our response to your deletion request.

8.5 Deletion from Third-Party Sub-Processors

- **Cloud infrastructure (AWS / GCP / Azure):** deletion propagated within 30 days per DPA terms.
- **AI provider (Anthropic):** data sent for AI processing is not stored beyond the processing request and is not used for model training, per our DPA.
- **Hiring companies:** if your data was shared with a hiring company (Section 6.3), you must contact that company directly to exercise deletion rights.

9. Your Rights as a Data Subject

9.1 Rights Under GDPR (EU/EEA residents)

- **Right of Access (Art. 15)** — obtain a copy of your data.
- **Right to Rectification (Art. 16)** — correct inaccurate data.
- **Right to Erasure (Art. 17)** — 'right to be forgotten'.
- **Right to Restriction (Art. 18)** — limit processing in certain circumstances.
- **Right to Data Portability (Art. 20)** — receive data in a machine-readable format.
- **Right to Object (Art. 21)** — object to processing based on legitimate interests.
- **Right not to be subject to automated decision-making (Art. 22).**

9.2 Rights Under CCPA / CPRA (California residents)

- **Right to know** — request disclosure of data collected, its sources, and third parties it is shared with.
- **Right to delete** — request deletion subject to certain exceptions.
- **Right to correct** — request correction of inaccurate personal information.
- **Right to opt-out of sale or sharing** — we do NOT sell or share your personal information for behavioural advertising. Submit requests to privacy@lightico.com.
- **Right to limit use of sensitive personal information (SPI)** — you may request limitation of

SPI use at any time.

- **Right to non-discrimination** — exercising your rights will not affect your service quality.

To submit a CCPA request, email privacy@lightico.com with subject line *California Privacy Request*. We respond within 45 days.

9.3 Rights Under Israeli Privacy Protection Law

- Right to access personal data held about you.
- Right to correct inaccurate data.
- Right to request deletion of data no longer required.
- Right to object to use of data for direct marketing purposes.

Contact us at privacy@lightico.com. You also have the right to lodge a complaint with your local supervisory authority (e.g. the European Data Protection Authorities, the Israeli Privacy Protection Authority, or the California Privacy Protection Agency).

10. Security Measures

We implement appropriate technical and organisational measures (GDPR Art. 32) to protect your personal data:

- Encryption in transit (TLS 1.2+) and at rest.
- Role-based access control (RBAC) — three access tiers: Admin (full platform access), HR (all candidate records), and Hiring Manager (restricted to their own open positions only).
- Regular security assessments and penetration testing.
- Data Processing Agreements with all cloud and AI sub-processors.
- Incident response procedures — data breaches notified to supervisory authorities within 72 hours (GDPR Art. 33) and to affected individuals where required.

11. Contacts & Complaints

For any privacy-related enquiry, data subject request, or complaint:

- **Email:** privacy@lightico.com
- **Data Protection Officer:** dataprotectionofficer@lightico.com
- **Address:** Bay Studios, Swansea, United Kingdom, SA1 8QB

12. Policy Compliance

This Policy has been created to ensure that the company operates in a way that is consistent with its values, goals, and legal obligations. Failure to adhere to this Policy may result in disciplinary action.

This Policy is reviewed annually or where significant change occurs.

privacy@lightico.com · Bay Studios, Swansea, UK, SA1 8QB