



LIGHTBEAM JOB APPLICANT PRIVACY NOTICE

Table of Contents

Table of Contents

1. Applicability
2. About Lightbeam as Data Controller
3. Personal Data We Collect
 - 3.1 Identity and Contact Information
 - 3.2 Recruitment and Employment Information
 - 3.3 Technical and Communication Data
 - 3.4 Background Verification Data
 - 3.5 Special Categories of Personal Data
4. How We Collect Your Personal Data
5. Purposes and Lawful Bases for Processing
6. Sharing Your Personal Data
 - 6.1 Within Lightbeam
 - 6.2 Third-Party Service Providers
 - 6.3 Other Disclosures
7. International Data Transfers
8. Data Retention
9. Data Security
10. Your Privacy Rights
 - 10.1 Additional Notice for California Residents
 - 10.2 Additional Notice for Applicants in India
 - 10.3 How to Exercise Your Rights
11. Automated Decision-Making and Profiling
12. Changes to This Notice
13. Contact and Grievance Redressal

Introduction

Lightbeam.ai, (hereafter referred to as “Lightbeam”, “we”, “us”, or “our”) is committed to protecting the privacy and security of your personal data. Lightbeam provides a data security, privacy and governance platform that helps organisations discover, classify, govern and protect sensitive data.

This Job Applicant Privacy Notice (**“Notice”**) describes how we collect, use, store, share, and protect personal data provided by or collected about you in connection with your application for employment at Lightbeam. It also describes the privacy rights available to you.

This Notice applies to all job applicants worldwide, including candidates who apply through our website (www.lightbeam.ai), third-party job boards, recruitment agencies, or by any other means. This Notice should be read together with Lightbeam’s general Privacy Policy, where applicable. This Notice does not form part of any contract of employment or engagement and does not create any contractual right or obligation.

1. Applicability

This Notice applies to personal data processed by Lightbeam in connection with recruitment, hiring, candidate evaluation, background verification, offer management, onboarding and related pre-employment activities.

Where a local law provides additional rights or protections, we will process your personal data in accordance with such local law.

2. About Lightbeam as Data Controller

For the purposes of applicable data protection laws, Lightbeam will generally act as the data controller, business or data fiduciary in respect of Applicant personal data, as it determines the purposes and means of processing such data. Where you apply for a role in a specific country, the relevant Lightbeam entity in that jurisdiction may act as data controller for that processing activity.

Contact details:

Compliance Officer

Lightbeam Inc.

4950 Hamilton Ave, Suite 202

San Jose, CA 95130, United States

Email: privacy@lightbeam.ai

Phone: [+353-899475808](tel:+353-899475808)

3. Personal Data We Collect

We collect and process the following categories of personal data about you during the recruitment process:

3.1 Identity and Contact Information

- Full name
- Home address, email address, and telephone number
- Date of birth (where required by law or to verify eligibility)
- Photograph (if voluntarily submitted)

3.2 Recruitment and Employment Information

- Curriculum vitae (CV), cover letter and portfolio materials
- Details of qualifications, skills, certifications and educational history
- Current and previous employment history, job titles and employer details
- Information about current and expected remuneration, benefits and notice period
- References and feedback from reference providers
- Right to work documentation and proof of identity (e.g., passport, national ID, work permit)
- Assessment results, test scores and interview notes

3.3 Technical and Communication Data

- Audio and video recordings of interviews conducted virtually
- Communications exchanged with our recruitment team
- Device and usage data if you use our online application portal

3.4 Background Verification Data

- Criminal records checks, to the extent permitted and required by applicable law
- Education and employment verification results
- Credit checks, only where legally permitted and relevant to the role

3.5 Sensitive Personal Data

We only process sensitive personal data where strictly necessary and permitted by law. This may include:

- Disability or health information, to make reasonable adjustments during the recruitment process
- Race or ethnic origin, solely for equal opportunities monitoring on an anonymised, aggregated basis
- Any financial information provided.

We will always seek your explicit consent or rely on another recognised legal basis before processing such data and we will inform you at the time of collection.

4. How We Collect Your Personal Data

We collect your personal data through the following means:

- Directly from you, via your application, CV, cover letter, online forms, interviews, assessments and correspondence
- From third parties, such as recruitment agencies, job platforms (e.g., LinkedIn), reference providers and background check vendors
- From publicly available sources, such as professional networking sites and public professional directories, to the extent permitted by applicable law
- Through our systems, including applicant tracking systems, video conferencing tools, and our website application portal

5. Purposes and Lawful Bases for Processing

We process your personal data only when we have a valid reason to do so. The table below sets out our main processing activities and the corresponding lawful basis on which we rely.

Purpose	CCPA/CPRA Purpose / Basis
Receiving, reviewing, and assessing your application	Business purpose: To process and evaluate your application, assess your qualifications, and determine your suitability for employment.
Arranging and conducting interviews and assessments	Business purpose: To conduct interviews, assessments, and other recruitment activities necessary to evaluate candidates.
Communicating with you about your application status	Business purpose: To communicate with you regarding your application, interviews, assessments, and recruitment process.
Verifying your right to work in the relevant jurisdiction	Compliance with legal obligations: To verify employment eligibility and comply with applicable federal, state, and local employment laws.
Conducting background and reference checks	Business purpose / compliance with legal obligations: To conduct background and reference checks where permitted or required by applicable law and to assess suitability for employment.
Issuing an offer letter and executing employment documentation	Business purpose: To prepare and administer employment offers and related employment documentation.

Maintaining recruitment records for legal claims	Business purpose: To maintain records necessary to establish, exercise, or defend legal claims and to comply with applicable record-keeping requirements.
Equal opportunities monitoring	Business purpose: To monitor and promote equal employment opportunities, diversity, and fair hiring practices, subject to applicable law.
Retaining your details in our talent pool for future roles	Business purpose: To retain candidate information and contact you regarding future employment opportunities that may be relevant to your qualifications. Where required by applicable law, the company will obtain consent before retaining or using information for this purpose.
Improving our recruitment processes through analytics	Business purpose: To analyze and improve recruitment processes, candidate experience, and hiring effectiveness, using aggregated, deidentified, or otherwise legally permissible information where appropriate.
Processing sensitive personal information (e.g., health, diversity)	Business purpose / permitted CPRA purpose: To process sensitive personal information where necessary for employment and recruitment administration, legal compliance, equal opportunity monitoring, workplace accommodations, or other purposes permitted under applicable law.

Where we rely on consent, you may withdraw it at any time by raising a request at <https://int.privacy-web.lightbeam-ai.com/dsr/form/69e905bd7b27dcf0d09aa33f> .

Withdrawing consent will not affect the lawfulness of any processing carried out before the withdrawal, nor processing carried out on a different lawful basis.

What happens if you do not provide your data

Providing your personal data is generally a necessary requirement for us to process your application. If you do not provide certain information when asked, we may be unable to assess

Where we rely on consent, you may withdraw it at any time by contacting <https://int.privacy-web.lightbeam-ai.com/dsr/form/69e905bd7b27dcf0d09aa33f> .

Withdrawing consent will not affect the lawfulness of any processing carried out before the withdrawal, nor processing carried out on a different lawful basis.

6. Sharing Your Personal Data

We share your personal data only as necessary and with appropriate safeguards in place.

Recipients include:

6.1 Within Lightbeam

- Hiring managers, interviewers and panellists involved in the recruitment process
- Human Resources, Legal, and Compliance teams
- Finance and Payroll teams, upon acceptance of an offer
- IT and Security teams, for system access provisioning

6.2 Third-Party Service Providers

We engage trusted vendors who process your data only on our documented instructions and under contractual obligations that meet applicable data protection standards:

- Applicant tracking system providers
- Background screening and verification companies
- Video interview and assessment platforms
- Recruitment agencies

6.3 Other Disclosures

- Regulatory authorities, law enforcement, or courts, where required by law or to establish, exercise, or defend legal claims
- Potential acquirers or investors, in the event of a merger, acquisition, or corporate restructuring, subject to equivalent confidentiality obligations

We do not sell, rent, or otherwise disclose your personal data to third parties for their own marketing purposes. For applicants in California: Lightbeam does not sell or share your personal information.

7. International Data Transfers

Lightbeam may process and transfer Applicant personal data across jurisdictions, including to countries where Lightbeam, service providers or recruitment partners operate.

Where required by applicable law, we will use appropriate safeguards for international transfers, such as standard contractual clauses, data protection agreements, adequacy mechanisms, transfer impact assessments, encryption and access controls.

You may request a copy of the relevant transfer mechanism by raising a request at <https://int.privacy-web.lightbeam-ai.com/dsr/form/69e905bd7b27dcf0d09aa33f>.

8. Data Retention

We retain your personal data only for as long as necessary to fulfil the purposes for which it was collected, and in accordance with our legal, regulatory, and business obligations. The following general guidelines apply:

1. if you are hired, relevant Applicant personal data may become part of your employment or contractor record and will be retained in accordance with Lightbeam's employee or contractor retention practices;
2. if you are not hired, we may retain your Applicant personal data for a reasonable period to consider you for future opportunities, maintain recruitment records, comply with law or defend legal claims;
3. where we retain your data for future opportunities based on consent, you may withdraw such consent at any time; and
4. when personal data is no longer required, we will delete, anonymise or securely archive it in accordance with applicable law and Lightbeam's retention practices.

9. Data Security

Lightbeam implements appropriate technical and organisational security measures to protect your personal data against unauthorised access, accidental loss, destruction, alteration, or disclosure. As a data security company, we hold ourselves to a high standard. Our measures include:

- Encryption of data in transit and at rest
- Role-based access controls and least-privilege access principles
- Regular security assessments
- Incident response and breach notification procedures
- Contractual data processing obligations with all third-party vendors

In the event of a personal data breach that poses a risk to your rights and freedoms, we will notify you and any relevant supervisory authorities as required by applicable law.

10. Your Privacy Rights

Depending on where you are located, you may have the following rights in respect of your personal data. We will respond to all valid requests promptly and in any event, within the timeframes required by applicable law.

- **Right of Access:** Request a copy of the personal data we hold about you.
- **Right to Rectification:** Request correction of any inaccurate or incomplete personal data.
- **Right to Erasure:** Request deletion of your personal data where it is no longer necessary for the purposes for which it was collected, subject to any legal retention obligations.

10.1 Additional Notice for California Residents

- **Right to Know:** Request disclosure of the categories and specific pieces of personal information we have collected, used, or disclosed about you in the preceding 12 months.
- **Right to Delete:** Request deletion of your personal information, subject to certain exceptions.
- **Right to Correct:** Request correction of inaccurate personal information we hold about you.
- **Right to Opt-Out of Sale or Sharing:** As noted above, Lightbeam does not sell or share your personal information.

We will respond to verifiable consumer requests within the timelines required by the CCPA. California law generally requires businesses to respond within 45 calendar days, with a possible 45-day extension where permitted.

10.2 Additional Notice for Applicants in India

- **Right to Information:** Obtain a summary of the personal data we process about you and the processing activities involved.
- **Right to Correction and Erasure:** Request correction of inaccurate personal data and erasure of data that is no longer needed for the purpose for which it was collected.
- **Right to Grievance Redressal:** Raise a grievance with our Privacy Officer and receive a response within the applicable timelines.

We will respond to verifiable consumer requests within the timelines required by the DPDP Act. The DPDP Rules require Data Fiduciaries to respond to requests within 90 days.

10.3 How to Exercise Your Rights

To exercise any of the rights listed above, you may raise a request at <https://int.privacy-web.lightbeam-ai.com/dsr/form/69e905bd7b27dcf0d09aa33f>

We may need to verify your identity before processing your request. There is generally no fee to exercise your rights. We reserve the right to charge a reasonable fee or decline to act on requests that are manifestly unfounded or excessive.

11. Changes to This Notice

We may update this Notice from time to time to reflect changes in applicable law, our business operations, or our recruitment practices. The most current version will always be available at www.lightbeam.ai. Where changes are material, we will take reasonable steps to notify you, for example by email if we hold your contact details. We recommend checking this page periodically.

13. Contact and Grievance Redressal

For questions, concerns, requests or grievances relating to this Notice or the processing of your Applicant personal data, please contact:

Compliance Officer

Lightbeam Inc.

4950 Hamilton Ave, Suite 202

San Jose, CA 95130, United States

Email: privacy@lightbeam.ai.

Phone: +1 (650) 2248706