

JobRays Global Privacy Policy

1. Introduction

JobRays (“JobRays,” “we,” “our,” or “us”) respects your privacy and is committed to protecting your personal data. This Privacy Policy explains how we collect, use, disclose, store, and safeguard your information when you use our websites, applications, and services (collectively, the “Services”).

By using JobRays, you consent to the collection and use of your personal data in accordance with this Privacy Policy. If you do not agree, you must discontinue use of the Services.

This Privacy Policy is designed to comply with global data protection frameworks, including:

- **European Union & United Kingdom:** GDPR (EU 2016/679) and UK GDPR.
 - **United States:** CCPA/CPRA (California), COPPA (children’s data), and FTC Act.
 - **Canada:** PIPEDA and Quebec Law 25.
 - **India:** Information Technology Act, 2000 and Digital Personal Data Protection Act, 2023.
 - **Singapore:** Personal Data Protection Act, 2012.
 - **Japan:** Act on the Protection of Personal Information (APPI).
 - **South Korea:** Personal Information Protection Act (PIPA).
 - **United Arab Emirates (UAE/Dubai):** Federal Decree-Law No. 45 of 2021 and DIFC Data Protection Law, 2020.
 - **Bangladesh:** ICT Act, 2006 and Digital Security Act, 2018.
-

2. Information We Collect

2.1 Personal Information You Provide

When you use JobRays, we may collect:

- Account details: name, email address, phone number, country/region.
- Credentials: login information and authentication tokens.
- Uploaded resumes, education history, employment history, certifications, and other career-related inputs.
- Career goals, target roles, salary preferences, and responses to Q&A forms.
- Billing details: subscription plan, payment method.

2.2 Automatically Collected Data

- Device data: IP address, device type, operating system, browser type, and version.
- Usage data: pages visited, features accessed, session duration, time stamps.
- Cookies and tracking: session cookies, analytics cookies, and pixels for performance and personalization.

2.3 Sensitive Data

Certain personal data provided by you may be considered “sensitive” under Applicable Law, including:

- Professional or educational background, certifications, or performance indicators.
 - Career goals, learning preferences, and progression insights.
- We collect and process such data only where necessary for delivering the Services and in compliance with privacy laws.

2.4 Children’s Data

- JobRays does not knowingly collect personal data from children under 16 (or the minimum digital consent age in their jurisdiction).
- For US residents under 13 (COPPA), verifiable parental consent is required before account activation.

3. How We Use Your Information

We use your information to:

3.1 Provide Services.

- Deliver personalized AI-powered career guidance, roadmaps, and insights.
- Process your uploaded resumes, career data, and preferences to generate outputs.
- Facilitate payments, subscriptions, and plan management.

3.2 Improve and Personalize.

- Enhance Services, algorithms, and AI outputs.
- Tailor recommendations to your learning style, goals, and career path.
- Analyze usage patterns to optimize user experience.

3.3 Communicate.

- Send service-related updates, security notices, and account alerts.
- Provide customer support and respond to inquiries.
- With your consent, send promotional messages, newsletters, and offers (opt-out available).

3.4 Security and Compliance.

- Detect, prevent, and investigate fraud, abuse, or unauthorized access.
- Enforce our Terms & Conditions.
- Comply with Applicable Law, regulatory requirements, and legal processes.

3.5 Legal Obligations.

- Maintain tax, accounting, and compliance records.
- Cooperate with regulatory authorities where required.

4. Insights & Anonymized Data

4.1 Creation of Insights.

JobRays may use your data in anonymized and aggregated form (i.e., stripped of personal identifiers) to generate insights, statistics, and benchmarks. Examples include:

- “Most in-demand certifications among Indian users in 2026.”
- “Average salary targets of Data Science professionals in the UK.”
- “Top trending skills among entry-level developers globally.”

4.2 Commercial Use of Insights.

We may share or license anonymized and aggregated insights with enterprises, partners, research organizations, or the public, for purposes such as:

- Identifying market trends.
- Supporting industry research.
- Helping training providers understand skill demand.

4.3 Data Safeguards.

- Insights are always anonymized and cannot be traced back to any individual.
- We never share resumes, emails, or identifiable career data without explicit consent.

4.4 No Sale of Personal Data.

JobRays does not sell, rent, or trade your personal data to third parties. Where Applicable Law (e.g., CCPA/CPRA) defines “sale,” JobRays confirms it does not engage in such practices.

4.5 Future Programs (Optional Opt-In).

If JobRays introduces programs where users may **opt in** to share their data with employers, recruiters, or training partners, such sharing will occur only with:

- Explicit, informed consent.
- Clear notice and controls in your Account settings.
- Full compliance with Applicable Law.

5. Legal Bases for Processing

Depending on your location, JobRays processes your personal data under the following legal grounds:

5.1 European Union & United Kingdom (GDPR, UK GDPR).

- **Consent** – when you opt in to communications or provide sensitive career data.
- **Performance of Contract** – to provide subscribed Services (roadmaps, recommendations).

- **Legitimate Interests** – for improving Services, anonymized analytics, and security, balanced against user rights.
- **Legal Obligation** – to comply with tax, accounting, AML/KYC, and regulatory duties.

5.2 United States (CCPA/CPRA, COPPA, FTC Act).

- “Business purposes” as defined under CCPA/CPRA.
- Users have the right to know, delete, and opt out of “sale” (JobRays does not sell personal data).
- For children under 13, COPPA requires verifiable parental consent.

5.3 Canada (PIPEDA, Quebec Law 25).

- Consent, contractual necessity, and compliance with Canadian privacy laws.
- Rights to access, correction, and withdrawal of consent.

5.4 India (DPDP Act 2023, IT Act 2000).

- **Consent** is the primary basis for processing.
- Limited processing without consent is permitted for legitimate purposes (service provision, compliance).
- Grievance redressal available via appointed Grievance Officer.

5.5 Singapore (PDPA).

- Processing with consent, for contractual necessity, or where exceptions apply (e.g., legitimate business interest).

5.6 Japan (APPI).

- Processing with user consent, or under lawful exceptions.
- Users may request disclosure, correction, suspension, or deletion.

5.7 South Korea (PIPA).

- Explicit consent for collection, use, and transfer of personal data.
- Additional safeguards for sensitive data.

5.8 United Arab Emirates (Federal Law No. 45 of 2021, DIFC Law).

- Consent, contractual necessity, and regulatory compliance.
- Additional protections for government-related or sensitive personal data.

5.9 Bangladesh (ICT Act, Digital Security Act).

- Consent-based processing, subject to national security and cyber regulations.
-

6. Payments & Financial Data

6.1 Payment Processing.

- Payments are handled by **authorized payment processors and acquiring banks**. JobRays does not store full payment card numbers.

6.2 PCI DSS Compliance.

- Our payment processors maintain **PCI DSS** compliance, including encryption, tokenization, and secure handling of cardholder data.

6.3 AML/KYC Compliance.

- Where required by law, JobRays and its processors may request additional documentation (e.g., identity, tax details) to comply with **Anti-Money Laundering (AML)** and **Know Your Customer (KYC)** obligations.

6.4 Currency and Tax.

- Fees are charged in USD by default, with local currency equivalents where supported.
- Invoices and tax receipts are issued from JobRays (Sole Proprietorship – Raghav Deora, India), unless local VAT/GST rules require otherwise.

6.5 Chargebacks & Fraud Prevention.

- JobRays may suspend or terminate accounts engaged in fraudulent activity.

7. Sharing of Data

7.1 Service Providers.

We may share your information with trusted service providers under binding contracts, solely for delivering and improving the Services. Categories:

- **Authorized payment processors and acquiring banks** (payments)
- **Cloud hosting, storage, and authentication providers**
- **AI/ML providers** (to generate outputs)
- **Analytics providers** (performance/usage)

7.2 Legal and Regulatory Authorities.

We may disclose data if required to:

- Comply with Applicable Law, court orders, or legal process.
- Cooperate with regulators or government authorities.
- Protect the rights, safety, and property of JobRays, users, or the public.

7.3 Business Transfers.

In the event of a merger, acquisition, restructuring, or sale of assets, your personal data may be transferred to the successor entity, subject to this Privacy Policy.

7.4 Partners (Optional Programs).

If JobRays launches programs where users opt in to share their profile with employers, recruiters, or training partners, we will:

- Obtain explicit consent.
- Provide notice and controls in your account settings.
- Ensure compliance with Applicable Law.

7.5 Exclusions.

We do **not** share your personal information with advertisers, data brokers, or unrelated third parties.

8. International Transfers

8.1 Global Operations.

JobRays operates internationally, and your data may be transferred to servers outside your country of residence, including the United States, European Union, India, and Singapore.

8.2 EU/UK Safeguards.

For transfers from the EU/UK to countries without an adequacy decision, JobRays relies on:

- **Standard Contractual Clauses (SCCs)** approved by the European Commission.
- Equivalent transfer mechanisms under UK GDPR.

8.3 Other Jurisdictions.

Where required by law (e.g., Singapore PDPA, Japan APPI, Korea PIPA, UAE Federal Law, India DPDP), JobRays ensures appropriate safeguards for cross-border transfers.

8.4 User Consent.

By using the Services, you consent to the transfer and processing of your data in jurisdictions where JobRays and its providers operate, subject to Applicable Law.

9. Retention

9.1 General Policy.

We retain personal data only for as long as necessary to:

- Provide Services and maintain your account.
- Comply with legal, tax, accounting, or regulatory requirements.
- Resolve disputes and enforce agreements.

9.2 User-Requested Deletion.

- You may request deletion of your personal data at any time by contacting legal@jobrays.io.
- We will delete or anonymize your data within legally mandated timeframes, unless retention is required for compliance.

9.3 Anonymization.

Where deletion is not possible (e.g., for system backups), we will anonymize data so it can no longer identify you.

9.4 Retention Periods.

- **Account data:** retained while your account is active.
 - **Billing records:** retained for up to 7 years (as required by tax laws).
 - **AI outputs and logs:** anonymized or deleted within a commercially reasonable timeframe.
 - **Children's data:** deleted immediately upon discovery of improper collection.
-

10. Security

10.1 Safeguards.

We implement administrative, technical, and physical security measures to protect personal data, including:

- Encryption of data in transit (TLS/SSL) and at rest (AES-256).
- Role-based access controls with least-privilege principles.
- Multi-factor authentication for staff with access to sensitive data.
- Regular vulnerability scanning, monitoring, and audits.

10.2 Third-Party Security.

Our service providers maintain industry-standard security certifications and compliance frameworks.

10.3 User Responsibilities.

- You are responsible for keeping your account credentials secure.
- JobRays is not liable for breaches caused by compromised user credentials.

10.4 No Absolute Guarantee.

While JobRays uses best-practice safeguards, no system is 100% secure. Users acknowledge the inherent risks of transmitting information online.

10.5 Incident Response.

- In the event of a personal data breach, JobRays will notify affected users and relevant authorities within legally mandated timeframes (e.g., **72 hours under GDPR**).
- Notifications will include: nature of the breach, affected categories of data, and mitigation measures taken.

11. Children's Data

11.1 Age Restrictions.

- JobRays is not directed at children under **16 years of age**, or the minimum digital consent age in their jurisdiction (13 in the US, 14 in South Korea, etc.).
- If you are under the applicable age, you may only use JobRays with parental/guardian consent.

11.2 COPPA (United States).

- For users under 13 in the US, JobRays requires **verifiable parental consent** before account activation.
- Parents may review, delete, or withdraw consent for their child's data at any time.

11.3 GDPR-K (European Union/UK).

- Under GDPR, parental consent is required for users under 16 (or a lower age permitted by local law, no lower than 13).

11.4 India (DPDP).

- Processing of children's data requires parental consent under the DPDP Act, 2023.

11.5 Parental Rights.

Parents/guardians may request deletion of their child's personal data by contacting **legal@jobrays.io**.

11.6 Improper Collection.

If JobRays becomes aware of personal data collected without proper consent, we will promptly delete such data.

12. Regional Rights

12.1 European Union & United Kingdom (GDPR, UK GDPR).

Users have the following rights:

- Access to their personal data.
- Rectification of inaccuracies.
- Erasure ("right to be forgotten").
- Restriction of processing.
- Data portability.
- Objection to processing (including direct marketing).
- Right to lodge complaints with their Supervisory Authority.

12.2 United States (CCPA/CPRA, COPPA).

- Right to know what categories of personal information we collect, use, and disclose.
- Right to request deletion of personal information (subject to exceptions).
- Right to opt out of “sale/share” of personal information (JobRays does not sell personal data).
- Right to equal service and non-discrimination.
- Additional COPPA protections apply for users under 13 (see Section 11).

12.3 Canada (PIPEDA, Quebec Law 25).

- Right to access personal data.
- Right to correction.
- Right to withdraw consent.
- Quebec Law 25 grants enhanced transparency and portability rights.

12.4 India (DPDP Act, IT Act).

- Right to consent-based processing.
- Right to access and correction.
- Right to nominate a representative for exercising rights in case of incapacity.
- Right to grievance redressal (Grievance Officer details in Section 13).

12.5 Singapore (PDPA).

- Right to request access and correction of personal data.
- Right to withdraw consent at any time, subject to legal obligations.

12.6 Japan (APPI).

- Right to disclosure, correction, suspension of use, and deletion of personal data.
- Restrictions on overseas transfers without adequate safeguards.

12.7 South Korea (PIPA).

- Strong consent requirements for collection, use, and overseas transfer.
- Right to access, correction, suspension, and deletion.

12.8 United Arab Emirates (Federal Law No. 45/2021, DIFC Law).

- Rights to access, rectification, erasure, and objection.
- DIFC requires appointment of a Data Protection Officer for sensitive data.

12.9 Bangladesh (ICT Act, Digital Security Act).

- Rights to data security and protection under national cyber laws.
- Government may require disclosure in cases of national security.

12.10 Other Jurisdictions.

Users outside these regions may have rights under their local data protection laws. JobRays will comply with mandatory requirements in such jurisdictions.

13. Grievance & Redressal

13.1 India (DPDP Act, Consumer Protection E-Commerce Rules).

- JobRays has appointed a **Grievance Officer** for Indian users.
- Complaints will be acknowledged within **48 hours** and resolved within **30 days**, as mandated by Indian law.
- Contact details of the Grievance Officer are published at jobrays.io/legal.

13.2 European Union & United Kingdom (GDPR, UK GDPR).

- Users may contact our designated **Data Protection Officer (DPO)** for GDPR inquiries, data access requests, or complaints.
- EU/UK users also retain the right to lodge complaints with their Supervisory Authority.

13.3 Other Jurisdictions.

- Users in Canada, Singapore, Japan, South Korea, UAE, and Bangladesh may also escalate privacy concerns to their respective Data Protection Authorities, where applicable.

13.4 Primary Contact.

For all privacy-related requests (access, correction, deletion, complaints), users may contact:

 legal@jobrays.io

14. Changes to Privacy Policy

14.1 Right to Update.

JobRays may update or revise this Privacy Policy from time to time to reflect:

- Changes in our Services or features.
- Updates in Applicable Law.
- Operational, technical, or security adjustments.

14.2 Notification of Changes.

- **Material changes** will be communicated via email or a prominent notice on our platform at least **30 days prior** to taking effect.
- **Minor updates** (e.g., administrative edits, clarifications) may take effect immediately upon posting.

14.3 Continued Use.


By continuing to use JobRays after the effective date of any changes, you accept the revised Privacy Policy. If you do not agree, you may discontinue use of the Services and request account deletion.

15. Contact Information

For questions, concerns, or legal notices regarding this Privacy Policy or your personal data, please contact:

JobRays Legal Team

 Email: legal@jobrays.io

 Website: jobrays.io/legal

 Registered Address: **JobRays (Sole Proprietorship – Raghav Deora), Prayagraj, Uttar Pradesh, India – 211001**