TROOGUE.AI

Privacy Policy

Effective date: 15 June 2026 | Last updated: 15 June 2026

Troogue Private Limited · CIN U62020KA2023PTC174477

Our commitment: Troogue uses interview and assessment data to provide assessments and improve its own capability-intelligence systems. We do not sell interview data or anonymised interview datasets as standalone data products, and we do not use interview data for personalised advertising.

Effective date: 15 June 2026 | Last updated: 15 June 2026

1. Scope and who is responsible

This Privacy Policy explains how Troogue Private Limited ("Troogue", "we", "us" or "our") collects, uses, shares, retains and protects Personal Data in connection with the Platform and Services. It applies to Troogers, Employers, customer representatives, website visitors, interview participants, reviewers and other individuals whose Personal Data we process.

Depending on the Service and contract, Troogue may act as an independent data fiduciary/ controller, a joint controller, or a processor/service provider acting on a customer's documented instructions. A customer agreement or just-in-time notice may provide additional details.

This Policy is intended to support compliance with applicable privacy and data-protection laws, including the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 (India), the UK GDPR and Data Protection Act 2018, the EU GDPR where applicable, and relevant US state privacy laws.

2. Definitions

- “Personal Data” means information about an identified or identifiable individual.
- “Sensitive Data” includes categories receiving enhanced legal protection, such as health, biometric identification, sexual orientation, religious beliefs, government identifiers or financial credentials, depending on applicable law.
- “Processing” includes collecting, recording, organising, analysing, using, sharing, storing, deleting or otherwise handling data.
- “Profiling” means automated processing used to evaluate or predict aspects relating to a person, including professional performance, skills, reliability, preferences or behaviour.
- “Anonymised Data” and “De-identified Data” have the meanings set out in the Terms.

3. Personal Data we collect

3.1 Account and identity information

Name, contact information, login credentials, age or date-of-birth confirmation, location, account type, organisation, identity-verification details and communication preferences.

3.2 Professional and profile information

Photograph, CV/resume, employment history, education, skills, certifications, portfolio, desired roles, rate, availability, work preferences, broad location and profile summary.

3.3 Assessment and interview information

Questions, answers, transcripts, audio/video recordings, code, files, screen or browser interactions, timing, device and technical data, completion events, proctoring and integrity signals, reviewer notes, assessment scores, classifications, recommendations and related inferences.

3.4 Employer and engagement information

Job descriptions, role requirements, candidate shortlists, interviewer feedback, communications, engagement status, project information, time or delivery records and customer support information.

3.5 Payment and compliance information

Billing address, invoices, tax identifiers and transaction references. Full payment-card data is generally processed by authorised payment providers and should not be stored by Troogue unless specifically disclosed.

3.6 Device, usage and security information

IP address, browser, operating system, device identifiers, cookie or analytics identifiers, access logs, pages and features used, referring pages, timestamps, crash logs and security events.

3.7 Communications and support

Emails, calls, chat messages, survey responses, complaints, feedback and other communications with Troogue or through Platform channels.

3.8 Information from authorised third parties

Information may come from Employers, recruitment or delivery partners, assessment reviewers, background-verification providers, professional networks, referrals, public professional sources and service providers, where lawfully obtained and relevant to the Services.

4. Information collected through AI-enabled interviews and assessments

When you participate in an assessment or interview, we may collect and analyse:

- audio/video recordings, text answers, transcripts and code or files submitted;
- the questions shown, answer sequence, timing, completion time and interaction events;
- technical, communication and role-related performance indicators;
- browser, screen, window-change, device and other integrity or proctoring signals where disclosed;
- scores, skill classifications, summaries, match indicators and other model- or reviewer-generated inferences; and
- feedback or observations from interviewers, reviewers, Employers or assessment administrators.

We use this information to administer assessments, generate and explain results, match people with opportunities, maintain integrity, detect fraud, resolve disputes, provide authorised reports and measure quality. Any use for general model improvement, benchmarking or capability-intelligence development is subject to section 7 below.

We will provide a recording notice before recording starts and obtain consent where required. Troogue does not use facial expressions, voice characteristics or other biometric signals to infer emotions, mental-health status, personality or sensitive personal characteristics in recruitment, assessment or workplace contexts. We do not use recordings for biometric identification unless the identity-verification or security purpose is separately disclosed, lawfully authorised and subject to appropriate safeguards.

5. Public and Employer-visible profiles

Where you enable Employer-only or public visibility, we may display approved professional information including your name, photograph, professional title, selected skills, experience summary, role classifications, “Troogue Assessed” status and availability. We provide visibility controls or another clear authorisation process.

A Public Profile may be accessible without login. Search-engine indexing is a separate optional choice and will be enabled only where you separately select it. Where indexing is not selected, Troogue will apply reasonable technical measures, such as noindex directives and exclusion from public sitemaps. We will not intentionally publish direct contact details, government identifiers, residential address, full recordings or detailed assessment answers without separate permission or another lawful basis.

You may change profile-visibility or indexing choices and may request correction, restriction or removal from future display. Technical measures cannot prevent every independent copy. If

indexing was previously enabled, search-engine caches and copies outside our control may take additional time to disappear.

6. Why we use Personal Data and our legal bases

Purpose	Examples	Typical legal basis
Provide and administer the Services	Create accounts and profiles; run interviews and assessments; generate reports; provide matching, deployment, communication and support.	Performance of a contract; steps requested before a contract; consent where required.
Profile visibility	Show approved information to Employers or the public based on selected settings.	Consent or affirmative user choice; performance of the requested Service.
Assessment integrity and security	Detect impersonation, fraud, cheating, abuse, unauthorised access and technical threats.	Legitimate interests; legal obligations; contract; consent where required.
Analytics and improvement	Measure reliability; improve usability, scoring, matching, skills taxonomies, integrity controls and model performance.	Legitimate interests where permitted; consent where required; use of Anonymised Data.
Customer and account administration	Billing, invoicing, notices, account management and support.	Contract; legal obligation; legitimate interests.
Legal and compliance	Respond to lawful requests, enforce rights, investigate claims and meet statutory obligations.	Legal obligation; legitimate interests; establishment or defence of legal claims.
Marketing	Send product or event communications and measure campaigns.	Consent where required; permitted business communications; opt-out available.

7. Model improvement and the Troogue intelligence layer

Troogue may use interview, assessment, profile, engagement and Platform information to develop and improve its capability intelligence, assessment systems, scoring methodologies, skill taxonomies, capability graphs, matching, integrity tools, benchmarks, analytics, artificial-intelligence models and workforce-intelligence products.

We may review identifiable Assessment Data where reasonably necessary to conduct, secure, explain or validate the specific assessment, investigate integrity concerns, provide authorised reports and support, or resolve a complaint or dispute. We do not use raw identifiable audio/video recordings, direct identifiers or identifiable full transcripts, answers or code to train reusable general models or benchmark datasets.

Before interview or assessment information is used for general model improvement, benchmarking or capability-intelligence development, we remove or transform direct identifiers, minimise the information used and apply de-identification or anonymisation safeguards. De-identified data remains Personal Data where it can reasonably be linked back to a person and continues to receive appropriate protection. Only Anonymised Data, aggregated statistics or non-identifying derived features are placed in reusable training or benchmarking datasets or retained without a fixed period.

We may derive job-related patterns such as response timing, answer structure and completeness, technical accuracy, coding approach, role terminology, communication clarity derived from transcripts, interaction events and assessment-integrity signals. We do not use these patterns for

personalised advertising or to infer emotions, mental-health status, personality or sensitive personal characteristics.

Where applicable law requires consent for any Personal Data processing used in a model-improvement preparation step that is not necessary to provide the requested Service, we will provide a separate, optional and unticked consent. Refusing or withdrawing that consent will not affect completion of the core assessment or existing opportunities.

We do not sell interview or assessment data, whether identifiable, de-identified or anonymised, as a standalone data product. We do not use interview data for third-party targeted advertising. We may make commercial use of models, methodologies, benchmarks, aggregated statistics and Anonymised Data products that do not identify an individual.

We apply controls intended to limit access, remove unnecessary identifiers, test outputs and reduce the risk that a model memorises or reproduces Personal Data. No technical system is risk-free, and we respond to credible privacy or security concerns in accordance with applicable law.

8. Automated processing, profiling and human review

Troogue uses automated and AI-assisted systems to generate classifications, scores, summaries, integrity flags, recommendations and matching indicators. Outputs may support human decision-makers. Unless clearly disclosed and legally permitted, Troogue does not intend an automated output to be the sole basis for a final hiring or engagement decision that has a legal or similarly significant effect.

Where applicable, you may request meaningful information about the main factors considered, correct inaccurate input data, challenge a materially adverse outcome and request human review. We may withhold information that would compromise security, intellectual property, assessment integrity or another person's rights, while still providing an appropriate explanation.

We may evaluate assessment performance across groups and investigate credible bias or fairness concerns. We do not guarantee that every automated output will be error-free or unbiased.

9. How we share Personal Data

We may disclose Personal Data only as reasonably necessary for the purposes in this Policy, including to:

- authorised Employers, customers and their interviewers or reviewers, consistent with visibility settings and the Service requested;
- Troogue employees, affiliates, consultants and authorised human reviewers who require access;
- service providers supporting hosting, storage, security, communications, video, transcription, proctoring, analytics, payments, customer support, background verification and AI infrastructure;
- professional advisers, auditors, insurers, banks and potential investors or acquirers under appropriate confidentiality protections;
- government, regulatory, judicial or law-enforcement authorities where legally required or reasonably necessary to protect rights and safety; and
- another entity involved in a merger, financing, reorganisation, acquisition or sale, subject to appropriate confidentiality and continuity protections.

Service providers may use Personal Data only to provide contracted services or as otherwise permitted by law. Employers that independently use or retain data may have their own privacy obligations and notices.

Our material service-provider categories may include cloud hosting and storage, video and communications, transcription, assessment and proctoring tools, security and fraud prevention, analytics, customer support, payment processing and professional advisers. We contractually require providers to use Personal Data only for authorised purposes and to apply appropriate confidentiality and security safeguards.

10. No sale of interview data and advertising practices

Troogue does not sell or rent identifiable interview, assessment or profile data for money. We do not allow third parties to use interview data for their own targeted advertising. Website analytics or marketing cookies, if used, will be described in a cookie notice and consent mechanism where required.

Certain privacy laws define “sale” or “sharing” broadly. Where applicable, we will provide legally required opt-out mechanisms and honour recognised preference signals to the extent required.

11. International transfers

Troogue, its customers and its contracted service providers may process Personal Data in India and other countries where they operate. These countries may have different data-protection laws. Where cross-border safeguards are required, we use contractual, organisational and technical measures appropriate to the relevant law and transfer risk, such as approved contractual clauses, transfer assessments, access controls and data minimisation.

12. Retention and deletion

We retain Personal Data for as long as reasonably necessary to fulfil the purposes described in this Policy, provide and improve the Services, maintain the integrity and history of assessments, support Troogers and Employers, comply with contractual and legal obligations, resolve disputes, prevent fraud and misuse, and establish, exercise or defend legal claims.

The period for which we retain information may vary depending on:

- the nature, volume and sensitivity of the information;
- whether your account, profile, assessment, application or engagement remains active;
- whether the information continues to be used for matching, professional opportunities, assessment history, comparability or validity;
- the requirements of an Employer, customer engagement or signed agreement;
- the need to investigate suspected fraud, misconduct, security incidents or unauthorised assistance;
- the need to evaluate, validate, secure and improve our assessment systems, models and intelligence systems;
- any complaint, review, dispute, investigation or legal proceeding; and
- applicable legal, regulatory, tax, accounting, audit and contractual requirements.

Information collected through interviews and assessments - including recordings, transcripts, responses, code submissions, assessment results, integrity signals and related records - may be retained for as long as reasonably required to provide the Services, maintain assessment history, support matching and hiring processes, respond to assessment challenges, verify assessment integrity, improve and validate our systems, and meet our contractual or legal obligations.

We periodically review the Personal Data we retain. When Personal Data is no longer reasonably required for the purposes for which it was collected or otherwise lawfully processed, we will delete it, securely dispose of it or irreversibly anonymise it, subject to applicable law and legitimate record-keeping requirements.

Where you request deletion of your account or withdraw consent for an optional processing activity, we will stop using the relevant Personal Data for that activity and delete or anonymise it within a reasonable period, unless continued retention is reasonably necessary to complete an ongoing assessment, application or engagement; comply with law or an enforceable contractual obligation; support fraud prevention, security, audit or assessment integrity; resolve a complaint, dispute or legal claim; or process the information under another lawful basis permitted by applicable law.

Deletion of an account does not necessarily require immediate deletion of every record associated with that account. We may retain limited records where reasonably necessary for compliance, audit, security, fraud prevention, dispute resolution and legal-claim purposes. Personal Data contained in backups may remain until those backups are securely overwritten or deleted through our normal backup-rotation processes.

Information that has been irreversibly anonymised so that it can no longer reasonably identify you is no longer treated as Personal Data. Troogue may retain and use such anonymised or aggregated information, including datasets, patterns, benchmarks, statistical insights and model outputs, without a fixed retention period for research, analytics, service improvement, model development and workforce-intelligence purposes. We prohibit attempts to re-identify such information.

13. Security

We use reasonable and proportionate technical and organisational safeguards, which may include encryption in transit and at rest, access controls, authentication, logging, secure development practices, vulnerability management, vendor due diligence, confidentiality obligations, backups and incident-response procedures.

No method of transmission or storage is completely secure. Users must protect credentials, devices and access links and promptly report suspected compromise.

14. Data breaches

We maintain procedures to detect, assess, contain and respond to Personal Data breaches.

Where the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 apply, we will notify the Data Protection Board of India and each affected Data Principal of a personal data breach in the manner and within the timelines prescribed under those Rules, including notification to affected Data Principals without undue delay. To the extent then known, our notification will describe the nature and likely consequences of the breach, the measures we have taken or propose to take to mitigate it, safeguards you can take to protect yourself, and a contact point for further information.

Where other laws apply, we will also notify affected individuals and the relevant supervisory or governmental authorities within the timelines and in the form those laws require.

15. Your rights

Depending on applicable law and our role, you may have rights to:

- access or obtain a summary or copy of your Personal Data;

- correct inaccurate or incomplete Personal Data;
- delete Personal Data in applicable circumstances;
- withdraw consent, without affecting processing already lawfully performed;
- restrict or object to certain processing;
- receive portable data where applicable;
- opt out of certain targeted advertising, sale/sharing or profiling where required;
- request human review of certain solely automated significant decisions;
- nominate another person to exercise rights where permitted under Indian law; and
- complain to Troogue and, where the Indian framework applies, to the Data Protection Board of India (with appeals to the Telecom Disputes Settlement and Appellate Tribunal), or to another competent data-protection authority.

To protect privacy and security, we may verify identity and authority. Rights may be limited by law, another person's rights, security, legal privilege, assessment integrity or our role as a processor. Where Troogue processes data solely for a customer, we may direct the request to that customer.

16. Consent and withdrawal

Where we rely on consent, the request will describe the relevant data and purpose in clear language. Consent is voluntary unless the data is necessary to provide a requested Service.

Optional choices, including Public Profile visibility, search-engine indexing and any optional Personal Data processing for model improvement, will be separately presented, will not be pre-selected, may be refused without losing the core assessment service, and may be withdrawn independently.

You may withdraw consent through account controls or by contacting us. Withdrawal applies prospectively and may mean that an optional feature can no longer be provided. It does not require us to reverse processing already lawfully completed or delete information that has already been irreversibly anonymised.

17. Cookies and analytics

We use necessary cookies for login, security, consent management and core functionality. Optional functional, analytics and marketing technologies are disabled until consent is obtained where required. You can accept, reject or customise optional categories and change your choice at any time through the cookie preference centre.

Our Cookie Policy contains the current provider and cookie inventory, purposes, categories, typical durations and available controls. The live cookie preference centre shows which optional integrations are active on the relevant Platform surface.

18. Children

The Services are intended for adults aged 18 or over. We do not knowingly offer candidate or Employer accounts to children. If we learn that Personal Data was collected from a child contrary to this Policy, we will take appropriate steps to delete or restrict it.

19. Third-party links and customer-controlled processing

The Platform may link to third-party sites or integrate with customer systems. Their privacy practices are governed by their own notices. Where an Employer provides or controls an

assessment, role or candidate list, that Employer may determine some processing purposes and should provide its own privacy information.

20. Changes to this Policy

We may update this Policy to reflect legal, product, security or business changes. We will post the revised version and effective date. For material changes, we will provide additional notice and obtain renewed consent where required.

21. Contact, grievances and requests

Troogue Private Limited is registered in India with CIN U62020KA2023PTC174477.

Registered office: No. 517/35, 1st Main Road, 41st Cross, 8th Block, Jayanagar West, Bangalore South, Bengaluru, Karnataka 560070, India.

Grievance Officer and Data Protection Contact: Madhu Peravalli, Founder & CEO. Email: madhu.peravalli@troogue.ai.

Requests should include sufficient information to identify the account or assessment and the action requested. We will acknowledge and respond within the period required by applicable law and may ask for identity verification. If you are not satisfied with our response and the Indian data-protection framework applies, you may escalate your grievance to the Data Protection Board of India.

22. Additional information for the UK, EEA and Switzerland

Where the UK GDPR or EU GDPR applies, Troogue will identify an appropriate lawful basis, apply data minimisation, provide required transparency, support data-subject rights and use appropriate transfer safeguards. Individuals may complain to their local supervisory authority.

Special-category data will not be intentionally inferred or processed unless a lawful condition applies. Solely automated decisions producing legal or similarly significant effects will be used only where permitted and with applicable safeguards, including information, contestation and human intervention rights.

Where applicable law requires Troogue to appoint a local representative or Data Protection Officer, the relevant contact details will be provided in an applicable regional notice or through the contact above.

23. Additional information for US residents

Residents of certain US states may have rights to access, correct, delete or obtain a copy of Personal Data and to opt out of sale, targeted advertising or certain profiling. Troogue does not sell interview or assessment data, whether identifiable, de-identified or anonymised, as a standalone data product. Where a state law applies, we will provide required request and appeal mechanisms and will not unlawfully discriminate against a person for exercising privacy rights.

Requests and appeals may be submitted to madhu.peravalli@troogue.ai. We may verify identity and will respond within the period required by applicable law.