Kovon Global Private Limited
Reg Office: Flat No. C-602, Mana, Uber Verdant Phase 2, Carmelram, Bangalore, Bangalore South, Karnataka, India, 560035

CIN: U62099KA2025PTC204920

Data Privacy and Candidate Data Protection Policy

Kovon Global Private Limited | Level 1 Board Policy

Policy owner	CEO
Operational support	Head of People, CTO / Security Owner and relevant functional heads
Approving authority	Board of Directors
Effective date	1 April 2026
Version	1.0
Review frequency	Annual, or earlier if required by law, breach, audit finding, product change, AI-tool deployment or Board direction
Primary jurisdiction	Bengaluru, India
Privacy contact	privacy@kovon.io
Applies to	Employees, interns, contractors, candidates, clients, vendors, website users, app users, placement partners and agency workers
Related policies	Corporate Policy Governance Framework; Code of Conduct and Ethics Policy; Whistleblower and Non-Retaliation Policy; Information Security Policy once adopted

Privacy standard

Kovon must collect, use, share, retain and delete personal data only for lawful, fair, transparent and business-necessary purposes. Candidate and worker data must be treated as confidential business-critical information.

1. Purpose

Kovon Global Private Limited ("Kovon" or the "Company") adopts this policy to protect personal data handled through its recruitment, employment, workforce management, client, vendor, website, application, global mobility and business operations.

This policy is intended to align Kovon's practices with applicable Indian privacy law, including the Digital Personal Data Protection Act framework as applicable, and with responsible data governance standards expected of a recruitment and employment technology business.

2. Scope

This policy applies to personal data relating to employees, interns, contractors, candidates, clients, vendors, website users, app users, placement partners, agency workers and other identifiable individuals whose data is processed by or for Kovon.

It applies to data handled in Kovon HRMS, ATS, Google Workspace, Microsoft 365, WhatsApp, Excel / Sheets, CRM, cloud databases, third-party payroll tools, background verification vendors and any approved or unapproved system where Kovon personal data is stored or transmitted.

3. Definitions

Personal data means any data about an individual who is identifiable by or in relation to such data, whether directly or indirectly.

Processing includes collecting, recording, organising, storing, using, sharing, disclosing, transferring, analysing, retaining, deleting or otherwise handling personal data.

Candidate data means personal data collected or generated in connection with sourcing, assessment, recruitment, selection, placement, global mobility, onboarding or candidate support.

High-risk data means data that may create increased harm if misused, including government IDs, financial data, health data, biometric data, criminal or background verification data, caste or religion data, disability information and family or dependent details.

4. Data Categories

Category	Examples	Controls
Candidate identity and contact	Name, phone, email, resume, work history, education.	Collect only for recruitment, matching, communication and lawful hiring purposes.
Recruitment assessment	Interview notes, assessment results, salary expectations, offer details.	Limit access to authorised hiring, recruitment, HR and decision-making personnel.
Government and mobility documents	ID documents, Aadhaar, PAN, passport, visa documents.	Use only where necessary; apply restricted access, secure storage and deletion controls.
Verification and risk data	Background verification data, criminal check data, reference information.	Use approved vendors; collect only with appropriate notice/consent or lawful basis.
Employment and payroll data	Bank details, family/dependent details, attendance, benefits, compensation.	Use for employment administration, payroll, statutory compliance and benefits.

Sensitive personal context	Health/medical records, disability information, caste/religion where legally required.	Collect only when legally required or clearly necessary; restrict access and retention.
Digital and usage data	Website/app use, system logs, device, access and security records.	Use for security, service delivery, analytics and compliance with notice and safeguards.

5. Privacy Principles

Lawful purpose: Personal data must be processed only for a lawful, specific and legitimate business purpose.

Transparency: Individuals should receive clear notice of what data is collected, why it is used, how it may be shared and how rights can be exercised.

Data minimisation: Teams must collect only the data reasonably needed for the stated purpose.

Purpose limitation: Data collected for one purpose must not be reused for an incompatible purpose without appropriate legal basis, notice or consent.

Accuracy: Kovon should take reasonable steps to keep personal data accurate and up to date where decisions rely on it.

Storage limitation: Data must not be retained longer than required for business, legal, audit, dispute, security or compliance purposes.

Security: Personal data must be protected by appropriate technical, organisational and contractual safeguards.

Accountability: Kovon must be able to evidence notices, consents where needed, access controls, vendor controls, retention, rights handling and breach response.

6. Permitted Processing Purposes

Kovon may process personal data for legitimate and lawful purposes, including:

1. candidate sourcing, screening, matching, assessment, interviewing, selection and offer management;
2. employment, internship, contractor and agency-worker onboarding and administration;
3. background verification, reference checks, identity checks, payroll, benefits and statutory compliance;
4. global mobility, immigration, visa, relocation and overseas employer or client coordination;
5. client, vendor, placement partner and business relationship management;
6. website, application, CRM, support and communication operations;

7. security monitoring, access management, fraud prevention, incident response and audit;
8. legal claims, regulatory compliance, internal investigations and dispute handling;
9. analytics, product improvement and AI-supported matching or workflow automation, subject to safeguards.

7. Notice, Consent and Legitimate Uses

Kovon must provide appropriate privacy notices at or before the time personal data is collected, unless an exception applies. Notices should be concise, accessible and aligned to the data subject group, such as candidates, employees, app users, website users or vendors.

Where consent is required, it must be informed, specific, clear and capable of withdrawal. Withdrawal of consent may affect Kovon's ability to provide a service, continue a recruitment process or complete employment administration where the data is necessary.

Some processing may be necessary for employment, legal compliance, contractual performance, security, claims, investigations or other lawful uses. The Privacy Owner should determine the appropriate basis with legal support where required.

8. Candidate Data Protection

Candidate data is especially sensitive because it may affect employment opportunities, immigration pathways, compensation discussions and professional reputation. Kovon must handle candidate data with fairness, confidentiality and restraint.

10. Candidate data must be collected through approved channels and stored in approved systems wherever feasible.
11. Interview notes must be professional, job-related, factual and free from discriminatory or irrelevant comments.
12. Recruiters and hiring teams must not collect unnecessary personal, family, caste, religion, health, political, financial or biometric information unless legally required or clearly justified.
13. Candidate documents must not be shared through personal email, unauthorised messaging groups or unmanaged spreadsheets unless approved and secured.
14. Candidate data shared with clients, overseas employers, mobility vendors or background verification vendors must be limited to what is necessary for the purpose.
15. Candidates must not be charged improper payments, coerced into sharing unnecessary data or misled about how their data will be used.

9. High-Risk Data Controls

Aadhaar, PAN, passport, bank details, health/medical records, biometric data, criminal/background check data, caste/religion, disability information and family/dependent details require enhanced safeguards.

Control	Requirement
Need-to-collect test	Collect high-risk data only when necessary for a lawful business, employment, compliance, verification, payroll, benefits or mobility purpose.
Access restriction	Limit access to authorised HR, payroll, security, legal, finance, mobility or verification personnel on a need-to-know basis.
Storage	Store in approved systems with access controls; avoid unmanaged local downloads and personal devices.
Masking/redaction	Mask or redact identifiers where full data is not required.
Sharing	Share externally only with approved recipients under appropriate contractual, confidentiality and security controls.
Deletion	Delete, archive or anonymise when the retention period expires and no legal hold applies.

10. Children and Minors

If Kovon processes personal data of individuals under 18, including interns, apprentices, trainees or candidates, Kovon must apply guardian-consent and age-appropriate safeguards where required by law.

Kovon must not process children's personal data in a way that is detrimental to their well-being. AI profiling, behavioural monitoring or targeted communications involving minors require prior review by the Privacy Owner and CTO / Security Owner.

11. AI, Automation and Fairness

Kovon may use AI tools for resume screening, interview support, candidate matching, chatbot support, automated shortlisting or workflow assistance only with appropriate governance.

16. AI tools must be reviewed before use for privacy, security, bias, explainability, vendor terms and data retention risk.
17. Candidates should not be rejected solely by automated processing without appropriate human review where the decision is significant.
18. AI outputs must be treated as decision support, not unquestioned fact.
19. Sensitive or high-risk data must not be entered into public or unapproved AI tools.
20. AI tools must not be used to infer caste, religion, health, disability, pregnancy, political views or other irrelevant protected characteristics.
21. Kovon should maintain records of approved AI tools, purposes, data categories, vendors and safeguards.

12. Access, Sharing and Cross-Border Transfers

Kovon may share personal data with overseas employers, global mobility vendors, immigration advisors, international clients, cloud servers outside India, cloud service providers, payroll providers, background verification vendors and other approved recipients where required for lawful business purposes.

Before sharing personal data outside India or with an overseas recipient, teams must confirm that the transfer is necessary, proportionate, covered by appropriate notice/consent or lawful basis, and subject to confidentiality, security and contractual controls.

Kovon must not transfer personal data to recipients or countries restricted by applicable law or government direction.

13. Vendor and Partner Controls

Vendors and partners that process personal data for Kovon must be assessed and contractually bound to protect data. This includes ATS providers, payroll vendors, cloud providers, background verification vendors, immigration advisors, CRM providers, AI tools and placement partners.

22. use personal data only for authorised purposes;
23. maintain appropriate security safeguards;
24. restrict onward sharing without approval;
25. notify Kovon promptly of data incidents;
26. support data-subject rights and deletion requests where required;
27. return, delete or securely dispose of data at the end of service, subject to legal retention.

14. Data Subject Rights and Requests

Individuals may contact privacy@kovon.io for privacy requests, including access, correction, deletion, consent withdrawal, grievance, nomination or other rights available under applicable law.

The CEO as Privacy Owner will oversee rights handling with Head of People support. Requests involving systems, security logs, deletion, vendor data or app/website data should include CTO / Security Owner support.

Kovon may verify identity before acting on a request and may decline, limit or defer a request where legally permitted, including for legal claims, statutory retention, fraud prevention, security, investigation, contractual obligations or rights of others.

15. Retention and Deletion

Record type	Retention standard
Unsuccessful candidate records	12 to 24 months, unless a longer period is needed for consented talent pool retention, legal claim, audit, dispute or legal hold.

Hired candidate / employee records	Employment period + 7 years, unless a longer statutory, tax, payroll, immigration, benefits, dispute or legal hold period applies.
Contractor / vendor records	Contract period plus 7 years, unless a longer legal, tax, audit, dispute or contractual period applies.
Interview notes	12 to 24 months unless the candidate is hired or the notes are needed for dispute, audit, investigation or legal hold.
Security logs and access records	As defined by the Information Security standard, legal requirement, incident need or audit requirement.
High-risk identity and verification documents	Retain only as long as necessary for verification, employment, mobility, compliance, audit, dispute or legal hold.

16. Security Requirements

Kovon must implement reasonable security safeguards to protect personal data from unauthorised access, disclosure, alteration, loss, misuse or destruction.

28. role-based access and periodic access reviews;
29. multi-factor authentication for sensitive systems where feasible;
30. secure password and credential practices;
31. approved storage locations and restrictions on personal devices or unmanaged downloads;
32. encryption or equivalent safeguards for sensitive data where feasible;
33. secure sharing practices and avoidance of unnecessary WhatsApp or spreadsheet sharing;
34. vendor security review for systems processing personal data;
35. staff training on privacy, phishing, data handling and incident reporting.

17. Personal Data Breach Response

A personal data breach includes unauthorised access, disclosure, loss, alteration, destruction, ransomware, phishing compromise, misdirected emails, exposed spreadsheets, credential misuse or vendor incident involving personal data.

Breach response is owned by the CTO / Security Owner and Privacy Owner, with CEO escalation. The Head of People must support breaches involving employees, candidates, contractors or agency workers.

Step	Action
Identify and contain	Secure systems, revoke access, preserve logs, stop unauthorised sharing and prevent further harm.

Assess	Identify data categories, affected individuals, systems, vendors, jurisdictions, risk level and likely harm.
Notify internally	Escalate to CTO / Security Owner, Privacy Owner, CEO, Head of People and Legal / Compliance as needed.
Notify externally	Notify affected individuals, regulators, clients, vendors or authorities where required by law or contract.
Remediate	Correct root causes, update controls, document decisions and report material issues to the Board.

18. Training and Acknowledgement

All covered persons with access to personal data must complete privacy and data-handling training appropriate to their role. Recruiters, HR, payroll, mobility, product, engineering, support and vendor-management teams should receive targeted training.

Acknowledgement of this policy is mandatory for employees, interns, contractors, agency workers and other covered persons with access to Kovon personal data.

19. Exceptions and Breaches

Exceptions to this policy must be approved under the Corporate Policy Governance Framework. No exception may permit unlawful processing, avoidable high-risk data collection, unauthorised AI use, concealment of a breach or sharing data without required safeguards.

Policy breaches may result in access restriction, retraining, disciplinary action, contract action, vendor action, termination, reporting to authorities or legal proceedings depending on severity and applicable law.

20. Review and Amendment

This policy will be reviewed annually by the CEO as Privacy Owner with Head of People and CTO / Security Owner support and submitted to the Board of Directors for approval of material changes.

Appendix A: Data Handling Checklist

36. Do we have a clear purpose for collecting or using this data?
37. Have we provided appropriate notice or obtained consent where required?
38. Are we collecting only what we need?
39. Is high-risk data genuinely necessary?
40. Is the data stored in an approved system with proper access controls?
41. Are we sharing only the minimum data with approved recipients?

42. Is a vendor, overseas transfer or AI tool involved?
43. Do we know the retention period and deletion trigger?
44. Would the data subject reasonably expect this use?
45. Have we escalated privacy or security uncertainty before acting?

Appendix B: Candidate Privacy Notice Minimum Content

46. identity and contact details of Kovon and privacy@kovon.io;
47. categories of candidate data collected;
48. purposes of recruitment, assessment, placement, mobility and communication;
49. recipients or recipient categories, including clients, overseas employers, vendors and mobility partners;
50. cross-border transfer notice where relevant;
51. AI or automated tool use where relevant;
52. retention period or retention criteria;
53. rights and grievance process;
54. consequences where required data is not provided.

Appendix C: Acknowledgement

I acknowledge that I have received or been given access to Kovon's Data Privacy and Candidate Data Protection Policy. I understand that I am expected to protect personal data, use approved systems, report suspected breaches promptly and comply with privacy, security, confidentiality and retention requirements.

Name	
Role / engagement type	
Department / function	
Signature / electronic acknowledgement	
Date	