Privacy Policy

Created On: September 15, 2025
Last Reviewed On: September 15, 2025

1. Introduction and Scope

1.1 About Wytmode Cloud Private Limited

Wytmode Cloud Private Limited ("Wytmode", "we", "us", or "our") is a technology company incorporated in India that designs and operates secure, privacy-centric software and services for global users, clients, candidates, employees, vendors, and partners. Our registered office is at #63, H Colony, 2nd Main, Indira Nagar, 1st Stage, Bengaluru (Karnataka, India) - 560038. This Privacy Policy explains, in comprehensive detail, how we collect, use, disclose, store, transfer, and protect personal data and professional or business data processed across our organization.

1.2 Coverage of Products and Services

This Policy applies to all processing activities undertaken by Wytmode and covers our enterprise division and SaaS products. Wytmode Workforce provides staffing, workforce augmentation, and related HR and compliance services to global clients. PlanInsta provides a web-based platform for business planning, assessments, and strategy enablement for entrepreneurs and enterprises. Wytmode Passwords Manager provides a zero-knowledge, end-to-end encrypted password management service for individuals and organizations. The Policy also applies to our corporate website, product websites, web applications, APIs, mobile or desktop clients (if any), and all related customer support and back-office operations.

1.3 Purpose of this Policy

The purpose of this Policy is to give every data subject a clear, authoritative, and exhaustive explanation of our privacy practices. It sets out why and how we process personal data, on what legal bases, for how long, with whom we share it, how we secure it, which international transfer mechanisms we rely upon, and how individuals can exercise their rights. Where product-specific practices differ, those distinctions are expressly stated to avoid ambiguity.

1.4 Legal and Regulatory Alignment (GDPR, CCPA, ISO 27001, etc.)

Wytmode designs its privacy program to comply with and, where commercially feasible, exceed the requirements of the European Union General Data Protection Regulation (GDPR), the United Kingdom GDPR and Data Protection Act, the California Consumer Privacy Act as amended by the CPRA (collectively "CCPA/CPRA"), the India Digital Personal Data Protection Act, 2023 (DPDP Act), and other applicable laws including Brazil's LGPD, Canada's PIPEDA, Singapore's PDPA, South Africa's POPIA, and analogous regimes worldwide. Our information security

controls are aligned to ISO/IEC 27001 principles and industry best practices, and our breach response, vendor governance, and records of processing are operated to meet recognized regulatory expectations.

1.5 Commitment to Users, Clients, and Partners

We commit to lawfulness, fairness, transparency, data minimization, purpose limitation, accuracy, storage limitation, integrity, confidentiality, and accountability. We do not sell personal data, and we do not share personal data for cross-context behavioral advertising without a valid legal basis, including consent where required. We continually review and improve our privacy and security posture and welcome questions at legal@wytmode.com or by phone at (+91) 8884557972.

2. Definitions and Key Terms

2.1 Personal Data

Personal Data means any information relating to an identified or identifiable natural person, including identifiers such as name, email address, phone number, identification numbers, online identifiers, geolocation data, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

2.2 Professional / Business Data

Professional or Business Data means information that relates to an individual's or organization's professional activities in connection with our Services, including resumes, employment history, skills matrices, project information, statements of work, business plan content, financial models supplied for planning, and records of professional interactions.

2.3 Sensitive Data

Sensitive Data means personal data subject to heightened protections under applicable law, which may include government identifiers, financial account information, precise geolocation, biometric identifiers, health information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning sex life or sexual orientation, or children's data as defined by law.

2.4 Data Subject

A Data Subject is any identified or identifiable natural person to whom the personal data relates, including clients' personnel, candidates, employees, contractors, platform users, and visitors to our websites and applications.

2.5 Controller and Processor

Wytmode acts as a Controller when it determines the purposes and means of processing personal data, for example in relation to our product users, candidates, employees, and marketing operations. Wytmode may act as a Processor when handling data strictly on behalf of a client under written instructions, such as certain workforce assignments or client-directed service engagements.

2.6 Third Parties and Sub-processors

Third Parties and Sub-processors are external entities engaged to provide services necessary to deliver and support our operations, including infrastructure, authentication, analytics, payment processing, HR and payroll systems, customer support tools, and security services. All such parties are bound by appropriate contractual safeguards, confidentiality obligations, and data protection terms commensurate with applicable laws.

3. Collection of Personal Data

3.1 Sources of Data Collection

We collect data directly from data subjects when they create accounts, complete forms, upload documents, communicate with us, enter into contracts, or use our Services. We collect data automatically through cookies and similar technologies when users access our websites and applications. We may also obtain data from clients, recruiting partners, background-screening providers, public sources, and service providers where, permitted by law and contract.

3.2 Data Collected via Wytmode Workforce

For Wytmode Workforce, we collect and process client contact details, business requirements, contractual documentation, invoicing information, and communications necessary to deliver engagements. For candidates and employees, we process identification documents, resumes, education and employment history, background screening results where, permitted, immigration and compliance information, payroll and benefits data, performance and attendance records, device or asset assignment, and any other information required by law or contract for lawful workforce management.

3.3 Data Collected via PlanInsta

For PlanInsta, we collect account information such as name, email address, and authentication data, together with business plan inputs, uploaded files, research notes, financial assumptions, generated reports, and usage telemetry relevant to feature performance and security. Where PlanInsta offers assessments or learning modules, we process responses, scoring outputs, and progress history to provide personalized results and maintain service integrity.

3.4 Data Collected via Passwords Manager

For Wytmode Passwords Manager, we purposefully collect the minimum personal data needed to run the service, typically an email address and authentication metadata managed through a secure identity provider. Vault contents such as passwords, usernames, URLs, secure notes, and custom fields are encrypted on the user's device before transmission and remain encrypted at rest with a zero-knowledge architecture. Wytmode has no technical ability to view, derive, or decrypt vault contents.

3.5 Data from Vendors, Partners, and Affiliates

We collect vendor and partner information including corporate details, tax and banking information for payments, points of contact, security and compliance attestations, and communications necessary to manage relationships. Where affiliates or recruitment partners introduce candidates or clients, we process the information they provide in accordance with this Policy and our contractual commitments.

3.6 Data from Websites, Apps, and Digital Platforms

We process telemetry such as device type, browser, operating system, IP address, timestamps, referrers, session identifiers, error logs, and interaction data to maintain availability, security, and performance. Where legally required, we obtain consent for analytics or marketing cookies and honor user choices, including applicable opt-outs and preference signals.

4. Purpose and Use of Data

4.1 Staffing, Workforce & Recruitment (Workforce)

We use Workforce data to source and evaluate candidates, conduct interviews, perform lawful background checks, onboard and pay employees, allocate personnel to client projects, administer benefits, manage performance, and fulfill contractual obligations to clients. We also use data to meet labor, tax, and social security requirements and to provide reporting and audit trails required by clients and regulators.

4.2 Business Planning & Assessments (PlanInsta)

We use PlanInsta data to generate investor-ready business plans, perform assessments, deliver analytics, provide user support, and improve platform features. Data is used to craft narrative, strategy, and financial projections as requested by the user, and to provide revision workflows, export functions, account management, and fraud prevention.

4.3 Password Storage & Security (Passwords Manager)

We use Passwords Manager account data to authenticate users, synchronize encrypted vaults, enforce security controls, and deliver customer support. We do not access vault contents, and all cryptographic keys necessary to decrypt vault entries remain under the user's control, never leaving the user context in a form accessible to Wytmode.

4.4 Client Relationship and Account Management

We use contact and account information to provide support, manage contracts and billing, respond to inquiries, deliver service notices, and measure service quality. We maintain records of communications and transactions for auditability, dispute resolution, and regulatory compliance.

4.5 Marketing, Analytics, and Communications

Where permitted by law, we use contact details to send service updates, security advisories, product announcements, and educational content. Marketing communications are conducted on a consent or opt-out basis as required in the recipient's jurisdiction, and recipients may withdraw consent or opt out at any time. Analytics are used to improve reliability and usability subject to consent requirements for non-essential cookies.

4.6 Security, Audit, and Compliance

We process data to secure our systems, investigate and prevent fraud and abuse, conduct logging and monitoring, perform vulnerability management, and comply with legal, tax, employment, financial, and regulatory obligations. We maintain auditable records of processing and implement controls aligned to ISO/IEC 27001 principles.

5. Lawful Basis for Processing

5.1 Contractual Necessity

We process data when necessary to enter into or perform a contract, including delivering services to clients, managing user accounts, paying employees, and fulfilling product features. Without this processing, we could not provide the Services requested by data subjects or clients.

5.2 Legal Obligations

We process data to comply with laws such as labor and employment regulations, tax and accounting rules, immigration and right-to-work requirements, anti-money-laundering obligations, and data protection statutes. Such processing is strictly limited to what the law requires or permits.

5.3 Consent-Based Processing

Where required, we obtain consent for activities such as certain marketing communications, specific categories of cookies, or processing of Sensitive Data. Consent may be withdrawn at any time, and withdrawal does not affect the lawfulness of processing carried out before withdrawal.

5.4 Legitimate Interests

We rely on legitimate interests to secure our Services, prevent fraud, improve and develop features, support customer needs, and operate our business efficiently. We balance these interests against the rights and freedoms of data subjects and implement safeguards to minimize privacy impact.

6. Data Retention and Minimization

6.1 Workforce Data Retention

Workforce data is retained for the duration of an engagement and thereafter for the period required by applicable law, limitation periods, or contractual audit requirements. Candidate profiles may be retained for a limited time to consider individuals for future roles, subject to consent or permissible interest and applicable opt-out rights.

6.2 PlanInsta User Data Retention

PlanInsta retains user accounts, business plan content, generated outputs, and related logs for as long as the account remains active or as necessary to provide and support the service. Upon account deletion or a valid erasure request, we delete or irreversibly anonymize data from active systems and backups within commercially reasonable timeframes consistent with legal obligations.

6.3 Passwords Manager Vault Data Retention

Passwords Manager retains encrypted vault data only for as long as an account exists. When a user deletes a vault item or an account, our systems trigger permanent erasure procedures designed to remove encrypted records from active systems, with cryptographic material remaining under user control. Consistent with service design, no plaintext is ever retrievable by Wytmode, and encrypted remnants in backups are subject to scheduled destruction policies.

6.4 Vendor and Partner Data Retention

Vendor and partner information is retained for the life of the relationship and for legally required retention periods for audit, taxation, and compliance. Where records are no longer necessary, they are securely deleted or anonymized.

6.5 Principles of Data Minimization

We collect only the data necessary for specified purposes, implement privacy-by-design in product and process development, and routinely review forms, fields, and logs to remove or avoid unnecessary personal data.

7. Data Sharing and Disclosures

7.1 Sharing within Wytmode Products & Divisions

We may share data internally among authorized teams solely for purposes consistent with this Policy, such as centralized security, billing, legal compliance, platform operations, and customer support. Internal access is governed by least-privilege and need-to-know principles.

7.2 Sharing with Clients, Vendors, and Partners

We share candidate and employee information with clients to the extent necessary to evaluate and manage assignments, subject to contractual confidentiality. We engage service providers for hosting, authentication, analytics, email delivery, HR and payroll, customer support, and security. Each provider is vetted and bound by contracts requiring confidentiality, security, and compliance with applicable laws.

7.3 Sharing with Sub-processors (e.g., Vercel, Clerk, Supabase)

Where relevant to particular Services, we may use Vercel & AWS for application hosting and deployment, Clerk, Supabase Authentication, AWS, and Auth0 for authentication and user management, and Supabase, NeonDB, AWS, Microsoft Azure and Google Cloud Platform for database hosting and management. These sub-processors act under our instructions and are contractually obligated to implement appropriate technical and organizational measures and to support compliance with data subject rights.

7.4 Sharing with Legal/Regulatory Authorities

We may disclose data when required by law, court order, or lawful governmental request, or to protect the rights, property, or safety of Wytmode, our users, or the public. We evaluate each request for scope and legality and challenge overbroad or improper demands where feasible.

7.5 Cross-Border Data Transfers

When data is transferred internationally, we implement appropriate safeguards such as Standard Contractual Clauses, adequacy decisions, binding agreements, or explicit consent, and we monitor legal developments to maintain the lawfulness and effectiveness of transfer mechanisms.

8. International Data Transfers

8.1 Intra-Wytmode Transfers

We may transfer data within Wytmode's global operations for hosting, support, security monitoring, and consolidated service delivery. Such transfers are governed by internal policies and agreements that require equivalent levels of protection regardless of location.

8.2 Transfers to Clients and Affiliates Globally

We may transfer data to clients, partners, or affiliates located in other countries to fulfill contractual commitments, operate cross-border teams, and provide support. We ensure that recipients are subject to confidentiality and data protection obligations consistent with this Policy.

8.3 Transfers Outside EEA / Other Regions

For transfers from the EEA, UK, or other jurisdictions with transfer restrictions, we rely on approved mechanisms such as the European Commission's Standard Contractual Clauses and UK International Data Transfer Addendum, along with supplementary measures where necessary to address local legal risks.

8.4 Safeguards (SCCs, Adequacy, Binding Agreements)

We continuously assess the legal landscape and apply appropriate safeguards, including reliance on adequacy decisions, execution of SCCs, and use of binding contractual protections that require recipients to implement robust security and respect data subject rights.

9. Security of Processing

9.1 Technical Measures (Encryption, Firewalls, Zero-Knowledge)

We design our systems to protect confidentiality, integrity, and availability through TLS for data in transit, encryption at rest, network segmentation, firewalls, intrusion detection and prevention, hardened configurations, logging, and rate limiting. Wytmode Passwords Manager employs a zero-knowledge architecture, with client-side encryption ensuring that Wytmode cannot decrypt user vault contents.

9.2 Organizational Measures (Policies, Governance, Staff Training)

We maintain written information security and privacy policies, conduct background screening where lawful, require confidentiality undertakings, and provide ongoing training and awareness programs. Governance is exercised by senior leadership, with oversight mechanisms that track risks, incidents, and remediation.

9.3 Access Controls & Identity Management

We enforce least-privilege access, role-based permissions, strong authentication, periodic access reviews, and segregation of duties. Administrative access to production systems is restricted and monitored, and service accounts are managed with credential rotation and secure secrets handling.

9.4 Incident Response & Breach Notification

We operate a documented incident response plan that includes detection, containment, eradication, recovery, and post-incident review. Where a breach creates a risk to individuals, we notify competent authorities and affected data subjects without undue delay and within statutory timelines, providing all required information and remedial guidance.

9.5 ISO 27001 & Continuous Improvement

Our controls are aligned to ISO/IEC 27001 principles, and we conduct periodic risk assessments, vulnerability management, internal audits, tabletop exercises, and corrective actions to drive continuous improvement of our security and privacy posture.

10. Rights of Data Subjects

10.1 Right of Access

Individuals have the right to obtain confirmation whether we process their personal data and to receive a copy along with information about the processing activities. We verify identity before fulfilling requests to protect privacy and security.

10.2 Right to Rectification

Individuals may request correction of inaccurate or incomplete personal data. We act promptly to rectify records and propagate corrections to relevant systems and vendors where appropriate.

10.3 Right to Erasure (Right to be Forgotten)

Individuals may request deletion of personal data where, permitted by law, including when data is no longer necessary, consent is withdrawn, or processing is unlawful. In Passwords Manager, account or entry deletion triggers permanent erasure workflows aligned with the service's zero-knowledge design.

10.4 Right to Restrict Processing

Individuals may request that we restrict processing while a dispute is resolved or where processing is contested. During restriction, we will store data but not otherwise process it except as permitted by law.

10.5 Right to Data Portability

Where applicable, individuals may request to receive their personal data in a structured, commonly used, and machine-readable format and to have it transmitted to another controller. For Passwords Manager, portability may be fulfilled through client-side export tools that do not involve Wytmode accessing plaintext vault contents.

10.6 Right to Object

Individuals may object to processing based on legitimate interests or to direct marketing at any time. We will cease such processing unless we demonstrate compelling legitimate grounds or are required to continue by law.

10.7 Rights Regarding Automated Processing

Where decisions producing legal or similarly significant effects are made solely by automated means, individuals have rights to meaningful information about the logic involved and to request human review where mandated by law. Wytmode does not engage in automated decision-making with such effects without appropriate safeguards.

10.8 Exercising Your Rights

Requests can be made by emailing legal@wytmode.com or by contacting us at (+91) 8884557972 or by mail at our registered address. We respond within the timelines prescribed by applicable law, normally within one month, and we may request additional information to verify identity and jurisdiction.

11. Cookies and Digital Tracking

11.1 Purpose of Cookies

We use cookies and similar technologies to provide essential functionality, maintain sessions, remember preferences, enhance security, measure performance, and understand how services are used to improve reliability and user experience.

11.2 Types of Cookies (Analytics, Functional, Marketing)

Essential cookies enable core features such as authentication and load balancing. Functional cookies remember preferences and improve usability. Analytics cookies help us understand usage patterns and error conditions, and marketing cookies support optional communications where permitted. Non-essential cookies operate only with the appropriate legal basis, including consent where required.

11.3 Managing Cookie Preferences

Users can manage cookie preferences through browser settings and, where provided, our consent management tools. We honor legally recognized signals and mechanisms in supported jurisdictions, and disabling certain cookies may affect the availability or performance of features.

12. Vendor and Sub-processor Management

12.1 Vendor Selection & Due Diligence

We select vendors based on technical competence, security and privacy controls, reliability, compliance posture, and contractual readiness. Due diligence includes questionnaires, document reviews, and risk assessments proportionate to the services provided.

12.2 Contractual Safeguards & DPAs

We require written agreements that include confidentiality, data protection terms, breach notification obligations, and audit or attestation provisions. Where vendors act as sub-processors, we execute Data Processing Agreements and flow down obligations consistent with applicable law.

12.3 Ongoing Monitoring & Reviews

We periodically review vendor performance and risk, monitor changes in ownership or geography, and reassess compliance evidence. Material issues trigger remediation plans or termination where necessary to protect data subjects and our Services.

13. Accountability and Governance

13.1 Roles and Responsibilities

Accountability for privacy resides with senior leadership and designated privacy and security personnel, with clear lines of responsibility for product teams, HR, finance, legal, and operations. All personnel are responsible for protecting data in accordance with this Policy.

13.2 Privacy Officers & DPO (where applicable)

Where a Data Protection Officer or equivalent is required, we appoint a qualified individual to oversee compliance, advise on obligations, monitor adherence, and serve as a point of contact for authorities and data subjects. Contact details are available upon request or as required by local law.

13.3 Internal Audits and Reviews

We conduct internal audits, risk assessments, and program reviews to evaluate control effectiveness, legal alignment, and incident readiness. Findings are tracked to resolution, and lessons learned inform updates to policies and procedures.

13.4 Records of Processing Activities

We maintain records of processing activities that describe purposes, categories of data, recipients, transfers, retention, and security measures, enabling us to demonstrate compliance and respond to regulatory inquiries.

14. Policy for Minors and Sensitive Data

14.1 Handling Special Category Data (Workforce HR, etc.)

We process Sensitive Data only when necessary and lawful, such as for employment, benefits, health and safety, or regulatory compliance in Workforce engagements. Such processing is subject to strict access control, purpose limitation, and enhanced security safeguards.

14.2 Children's Data (PlanInsta/Passwords Manager considerations)

Our Services are intended for adults and business users. We do not knowingly collect personal data from children below the minimum age required by applicable law, and accounts may not be created by individuals under that age without verifiable parental consent where permitted. If we learn that children's data has been collected contrary to this Policy, we will delete it promptly.

15. Complaints and Grievances

15.1 Submitting Complaints to Wytmode

We take privacy complaints seriously and encourage individuals to contact us first so we can attempt prompt resolution. Complaints may be submitted by email to legal@wytmode.com, by phone at (+91) 8884557972, or by mail to our registered address.

15.2 Escalation to Supervisory Authorities

If a concern remains unresolved, individuals have the right to escalate to a competent supervisory authority in their jurisdiction, such as an EU Data Protection Authority, the UK Information Commissioner's Office, the California Privacy Protection Agency, or the Indian Data Protection Board, as applicable.

15.3 Cooperation with Regulators

We cooperate with regulators, respond to inquiries, and implement remedial actions as required by law. We maintain records to demonstrate compliance and transparency in all regulatory engagements.

16. Updates to this Privacy Policy

16.1 Review Frequency

We review this Policy regularly and update it to reflect changes in law, technology, operations, and industry standards. Reviews include input from legal, security, and product stakeholders to ensure completeness and accuracy.

16.2 Communication of Changes

Material changes will be communicated through our websites, applications, or direct notices where appropriate. The "Last Updated" date will reflect the effective date of the revised Policy and continued use of the Services after that date signifies acceptance.

16.3 Version Control & Archiving

We maintain version control and archive prior versions to enable transparency and to evidence compliance over time. Upon request, we will provide access to relevant prior versions where legally appropriate.

17. Contact Information

17.1 Wytmode Corporate Contact Details

Wytmode Cloud Private Limited is located at #63, H Colony, 2nd Main, Indira Nagar, 1st Stage, Bengaluru (Karnataka, India) – 560038. Our switchboard for privacy matters is (+91) 8884557972.

17.2 Product-Specific Privacy Contacts

All product and service privacy inquiries, including for Wytmode Workforce, PlanInsta, and Wytmode Passwords Manager, may be directed to legal@wytmode.com. We route requests internally to the appropriate team while maintaining confidentiality and access control.

17.3 Data Protection Officer (if applicable)

Where law requires the appointment of a Data Protection Officer or equivalent, we will publish or provide the DPO's contact details for the relevant jurisdiction and ensure that the DPO is accessible to data subjects and supervisory authorities for all matters relating to the processing of personal data.