GDPR Compliance Statement

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

1. Introduction and Scope

Wytmode Cloud Private Limited ("Wytmode", "we", "our", or "us") is committed to protecting personal data in accordance with the General Data Protection Regulation (EU) 2016/679 ("GDPR") and equivalent laws in the United Kingdom and other jurisdictions. This statement summarizes our GDPR compliance posture across all business lines and products operated by Wytmode, including Wytmode Workforce, PlanInsta, and Wytmode Passwords Manager, as well as our public websites, authenticated applications, and associated customer support operations. It is intended to provide clear, concise assurance to customers, users, candidates, employees, vendors, partners, and regulators that we process personal data lawfully, fairly, and transparently, and that we maintain appropriate technical and organizational measures to safeguard the rights and freedoms of natural persons.

2. Controller and Processor Roles

Wytmode acts as a controller where we determine the purposes and means of processing, such as account administration for PlanInsta and Passwords Manager, candidate lifecycle management, marketing, and corporate compliance. Wytmode may act as a processor where we process personal data strictly on documented instructions from a client, for example in certain Wytmode Workforce engagements or white-label arrangements governed by a master services agreement and data processing agreement. Our contracts clearly specify the respective roles, subject matter, duration, nature and purpose of processing, types of personal data, categories of data subjects, security obligations, and the conditions under which we engage subprocessors.

3. Lawful Bases for Processing

We identify and document a valid lawful basis for every processing activity before it begins. Contractual necessity applies where processing is required to provide the services or to perform pre-contractual steps at a data subject's request. Legal obligation applies to processing mandated by law, including tax, employment, accounting, immigration, social security, and fraud prevention. Consent applies where required for non-essential cookies, certain marketing communications, or specific categories of data, and can be withdrawn at any time without detriment to prior lawful processing. Legitimate interests apply where we have a proportionate and reasonable interest in security, service improvement, product analytics, or business operations that is not overridden by the interests or fundamental rights of data subjects; legitimate interest assessments are performed and retained for audit.

4. Transparency and Notices

We provide accessible, plain-language privacy notices at or before the point of data collection. These notices describe our purposes, lawful bases, categories of recipients, retention periods, international transfer mechanisms, data subject rights, and complaint avenues. Product-specific notices are surfaced within Wytmode Workforce portals, PlanInsta interfaces, and Passwords Manager properties so users can understand precisely how their information is used in each context, and we keep notices updated as our processing evolves.

5. Data Minimization, Purpose Limitation, and Retention

We collect only data that is relevant and limited to what is necessary for stated purposes, and we do not repurpose personal data in ways that are incompatible with the original purpose without an appropriate legal basis. We maintain documented retention schedules that specify the duration or criteria used to determine retention for each record class. When retention ends, we securely delete or irreversibly anonymize data from active systems and backups within commercially reasonable time frames, taking account of statutory obligations and limitation periods.

6. Security of Processing and ISO/IEC 27001 Alignment

We implement layered technical and organizational controls consistent with Article 32 GDPR, including encryption in transit and at rest, hardened cloud infrastructure, role-based access control and least-privilege design, multi-factor authentication for administrative access, secure software development life cycle, vulnerability management and patching, logging and monitoring, and tested backup and recovery procedures. Our information security management practices are aligned to ISO/IEC 27001 principles, and we pursue continuous improvement through risk assessments, internal audits, corrective actions, and leadership oversight.

7. Product-Specific Security Posture

For Wytmode Workforce, personnel and candidate data are stored within controlled HR systems subject to access segregation, audit logging, and compliance with applicable employment and labor laws. For PlanInsta, user accounts, business plans, financial assumptions, and exports are protected with strong authentication, encrypted transport, server-side access controls, and retention rules that respect user choices. For Wytmode Passwords Manager, vault contents such as passwords and secure notes are encrypted on the client side before transmission and remain encrypted at rest under a zero-knowledge architecture; Wytmode has no technical ability to decrypt user vault contents and relies on secure session controls solely for authentication and service delivery.

8. Vendors, Sub-processors, and Article 28 Contracts

We select vendors and sub-processors after due diligence on their security, privacy, reliability, and regulatory posture, and we bind them with written agreements that include Article 28 obligations, confidentiality, breach notification, audit cooperation, and data localization or transfer safeguards where applicable. We maintain an up-to-date register of sub-processors for each product area and provide notice of material changes in accordance with contractual commitments.

9. International Data Transfers and Schrems II

Where personal data are transferred outside the European Economic Area or the United Kingdom, we implement appropriate safeguards under Chapter V GDPR. These include reliance on adequacy regulations where available, execution of the latest Standard Contractual Clauses with supplementary measures informed by transfer risk assessments, and, where relevant, the UK International Data Transfer Addendum. We periodically review legal developments and our technical and organizational measures to ensure that transferred data receive a level of protection essentially equivalent to that guaranteed within the EU/EEA.

10. Data Subject Rights and Request Handling

We support all rights under Articles 12–23 GDPR, including the rights of access, rectification, erasure, restriction, portability, and objection, and rights relating to automated decision-making. We verify identity in a proportionate manner before fulfilling a request, respond without undue delay and within one month unless an extension is justified, and document our responses for accountability. Where a request pertains to data we process as a processor, we promptly notify and assist the relevant controller in meeting its obligations. We never charge for rights requests unless permitted by law due to manifestly unfounded or excessive requests.

11. Special Category Data and Children

We process special category data only where strictly necessary and lawful, for example to meet employment or health and safety obligations in Wytmode Workforce or to support reasonable accommodations. Such processing is supported by appropriate legal bases and safeguards, including access restrictions, encryption, and enhanced retention controls. 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 we remove such data promptly upon confirmed notice.

12. Privacy by Design, DPIAs, and Governance

We embed privacy by design and by default into product and process development through structured reviews, data flow mapping, and minimization controls. We conduct data protection impact assessments (DPIAs) for high-risk processing and maintain remediation plans to reduce residual risk to acceptable levels. Governance is exercised

by senior leadership with defined roles and responsibilities, periodic reporting, and integration of privacy risks into enterprise risk management. We maintain up-to-date records of processing activities in accordance with Article 30 GDPR.

13. Incident Response and Breach Notification

We maintain an incident response plan that defines roles, escalation paths, evidence preservation, containment, eradication, and recovery procedures. If a personal data breach is likely to result in a risk to the rights and freedoms of natural persons, we notify the competent supervisory authority without undue delay and, where feasible, within seventy-two hours of becoming aware. When the breach is likely to result in a high risk to individuals, we also communicate the breach to affected data subjects without undue delay in clear and plain language, providing guidance to mitigate potential harm.

14. Cookies and Online Identifiers

Our use of cookies and similar technologies is governed by clear consent mechanisms and preference tools that comply with the ePrivacy Directive, PECR, GDPR, and other relevant laws. Strictly necessary cookies are used to deliver the services requested by the user, while analytics and marketing cookies operate only with a valid legal basis, including consent where required. Our Cookies Policy explains in detail the categories used, typical lifetimes, controls, and how we honor recognized preference signals where supported.

15. Training, Awareness, and Accountability

All personnel with access to personal data receive role-appropriate privacy and security training at onboarding and on a periodic basis. We reinforce responsibilities through policies, confidentiality obligations, acceptable use standards, and disciplinary consequences for violations. Accountability is demonstrated through documentation, audit trails, vendor oversight records, and continuous improvement actions tracked to closure.

16. Contact, Representatives, and Supervisory Authorities

Questions or requests regarding this statement or our GDPR compliance may be directed to legal@wytmode.com, by phone at (+91) 8884557972, or by mail to Wytmode Cloud Private Limited, #63, H Colony, 2nd Main, Indira Nagar, 1st Stage, Bengaluru (Karnataka, India) – 560038. Where required by law, Wytmode will appoint an EU or UK representative and, if applicable, a Data Protection Officer for specific processing contexts; details will be made available in product notices or upon request. Data subjects also have the right to lodge a complaint with a competent supervisory authority, without prejudice to any other administrative or judicial remedy.

17. Updates and Versioning

We review this GDPR Compliance Statement periodically and update it to reflect changes in law, guidance, technology, or our processing activities. Material updates will be communicated through our websites or in-product notices as appropriate, and the effective date will be revised accordingly. Continued use of our services following publication of an update signifies acknowledgment of the revised statement to the extent permitted by law.