

# PRIVACY POLICY

## *Innovation Disclosure & Management System*

Governing the Collection, Use, Storage & Protection of Personal and Innovation Data

Document Version 1.0 | Applicable to All Institutions & Stakeholders

*This Privacy Policy describes how the Company collects, processes, stores, shares, and protects personal data and innovation-related data submitted through the Innovation Disclosure & Management System (the "Platform") by academic institutions and their stakeholders. By using the Platform, the Institution and each Stakeholder consent to the practices described herein. This Policy is to be read together with the Platform's Terms & Conditions.*

## 1. Identity of the Data Controller

The Company — being the entity that owns, operates, and licenses the Platform — acts as the Data Controller in respect of personal data and innovation disclosure data processed through the Platform. The Company is responsible for ensuring that such data is processed in a lawful, fair, and transparent manner in accordance with applicable data protection laws, including but not limited to the Information Technology Act, 2000, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules"), and the Digital Personal Data Protection Act, 2023 ("DPDPA"), as applicable.

The Institution, in its capacity as the entity through which Stakeholders submit data, acts as a Data Fiduciary in relation to its Stakeholders' personal data and is responsible for obtaining all necessary consents and authorisations from Stakeholders before their data is submitted to or processed through the Platform.

## 2. Scope of This Policy

This Privacy Policy applies to:

- All personal data and innovation-related data submitted by Institutions and Stakeholders through the Platform, including through QR-code-based submission interfaces;
- Data generated by the Platform in the course of providing its services, including Analyst Assessments, workflow records, and platform usage data;
- Data shared with the Company by Institutions in connection with their subscription and use of the Platform.

This Policy does NOT apply to:

- Third-party websites or services linked from the Platform;
- Data collected by the Institution from its Stakeholders through its own independent systems or processes;
- Publicly available information that is not submitted through the Platform.

### 3. Categories of Data Collected

The Company collects and processes the following categories of data through the Platform:

Category of Data	Examples	Purpose
Institutional Identity Data	Institution name, address, registration details, authorised representative details	Platform onboarding, account management, subscription administration
Stakeholder Identity Data	Name, designation, department, employee/student ID, contact email, phone number	Disclosure attribution, assessment communication, access control
Innovation Disclosure Data	Title, description, technical details, diagrams, prototypes, claims, categories of IP sought, commercial potential	Assessment, classification, workflow management
QR Submission Metadata	Submission timestamp, device type, IP address, geolocation (where enabled), QR session ID	Record integrity, fraud prevention, audit trail
Assessment & Analysis Data	Analyst notes, classification, drafting quality tier, recommendations, assessment timestamps	Service delivery, institutional reporting
Platform Usage Data	Login activity, pages accessed, features used, session duration, error logs	Platform improvement, security monitoring
Communication Data	Emails, messages, support queries exchanged between users and the Company	Service support, dispute resolution, quality assurance
Billing & Subscription Data	Invoice details, payment references, subscription tier, renewal dates	Financial record-keeping, contractual obligations

#### **⚠ Special Category — Innovation Disclosure Data**

Innovation Disclosure Data is treated as confidential and commercially sensitive data by the Company. It is not classified as 'sensitive personal data' under current Indian law but is afforded equivalent or higher levels of protection given its potential intellectual property value. The Company applies strict access controls, confidentiality obligations, and security measures to all Innovation Disclosure Data.

### 4. Lawful Basis for Processing

The Company processes data on the following lawful bases:

- **Contractual Necessity:** Processing is necessary to perform the Platform services under the subscription agreement with the Institution.
- **Legitimate Interests:** Processing for platform security, fraud prevention, product improvement, and quality assurance, where such interests are not overridden by the rights of data subjects.
- **Consent:** Where specific processing activities require consent (such as use of data for anonymised research or marketing communications), the Company will obtain explicit consent from the relevant data subject prior to such processing.
- **Legal Obligation:** Processing where required by applicable law, court order, or regulatory authority.

## 5. How Data Is Used

---

### 5.1 Core Service Delivery

Data collected through the Platform is primarily used to:

- Process and manage Innovation Disclosures submitted by Stakeholders;
- Enable Patent Analysts to conduct preliminary assessments and issue Drafting Quality Classifications;
- Generate and communicate Assessment reports to the Institution;
- Maintain workflow records, submission histories, and institutional dashboards;
- Provide customer support and respond to institutional queries.

### 5.2 Platform Improvement & Research

Subject to appropriate anonymisation and aggregation, the Company may use data to:

- Improve the Platform's features, interface, and analytical capabilities;
- Conduct internal research on innovation trends within academic institutions (using only anonymised, non-attributable data);
- Train and evaluate AI-assisted tools used in the assessment process, using anonymised disclosure data only.

*The Company will never use identifiable Innovation Disclosure Data for any research, publication, marketing, or commercial purpose without the prior explicit written consent of the Institution and the relevant Stakeholder(s).*

### 5.3 Legal & Compliance Purposes

Data may be used to:

- Comply with applicable laws, regulations, and legal processes;
- Enforce the Platform's Terms & Conditions and protect the Company's legal rights;
- Prevent, detect, and respond to fraud, security incidents, or unauthorised access.

## 6. Data Sharing & Disclosure

---

### 6.1 Internal Access

Access to Innovation Disclosure Data and Assessment Data within the Company is restricted on a strict need-to-know basis. Only the following personnel have access:

- Innovation Analysts assigned to the specific Innovation Disclosure;
- Platform administrators responsible for technical maintenance and support;
- Senior management where required for quality assurance or escalated dispute resolution.

### 6.2 Third-Party Service Providers

The Company may share data with trusted third-party service providers who assist in operating the Platform, including:

- Cloud infrastructure and hosting providers (for data storage and platform operations);
- Cybersecurity and data protection vendors;
- Communication and notification service providers;

- Payment processing providers (for billing data only);
- Individual and Institutional Innovation Index scores shall be shared to such parties as essential and may fit in the process.

All third-party service providers are contractually bound to process data only as instructed by the Company, to maintain appropriate security measures, and not to use data for their own purposes.

### 6.3 Innovation Analysts

Innovation Analysts engaged by the Company to review Innovation Disclosures are required to execute confidentiality agreements as a condition of engagement. Such agreements prohibit analysts from disclosing, reproducing, or using Innovation Disclosure Data for any purpose other than the assessment for which they are engaged. However, the Institution acknowledges that analysts may be independent contractors and that the Company cannot guarantee identical contractual terms across all analyst engagements.

### 6.4 Disclosure Required by Law

The Company may disclose data — including Innovation Disclosure Data — where required by:

- A court order, subpoena, or other legally binding judicial or regulatory process;
- Applicable law or regulation, including reporting obligations;
- A lawful request by a government authority or law enforcement agency.

Where legally permissible, the Company will notify the Institution of such a request before disclosing data, to afford the Institution an opportunity to seek appropriate legal relief.

### 6.5 Business Transfers

In the event of a merger, acquisition, restructuring, or sale of the Company or its assets, Innovation Disclosure Data and personal data may be transferred to the acquiring entity, subject to equivalent or stronger data protection obligations being imposed on the acquirer. The Company will notify the Institution of any such transfer with reasonable prior notice.

### 6.6 No Sale of Data

*The Company does not sell, rent, lease, or otherwise commercially exploit personal data or Innovation Disclosure Data to any third party under any circumstance. This prohibition is absolute and is not subject to any opt-out mechanism — it is a foundational commitment of this Privacy Policy.*

## 7. Cross-Border Data Transfers

---

The Platform is primarily operated from India. Innovation Disclosure Data and personal data may be stored on cloud infrastructure located within India or in other jurisdictions depending on the Company's cloud service provider arrangements.

Where data is transferred outside India, the Company ensures that such transfer is undertaken only:

- To jurisdictions recognised as providing adequate data protection under applicable Indian law;
- Subject to appropriate contractual safeguards (such as standard contractual clauses or equivalent mechanisms); or
- With the prior informed consent of the relevant data subject, where required.

Institutions and Stakeholders who have concerns about cross-border data transfers may contact the Company's Data Protection contact (see Section 15) for specific information about where their data is stored and processed.

## 8. Data Retention

The Company retains data for no longer than is necessary for the purposes for which it was collected, subject to applicable legal obligations. The following retention schedule applies:

Data Category	Retention Period	Basis
Innovation Disclosure Content	3 years from date of submission	Legitimate interest; institutional record-keeping
Analyst Assessment Reports	3 years from date of issue	Legitimate interest; legal accountability
Stakeholder Identity & Contact Data	Duration of institutional subscription + 3 years	Contractual necessity
Platform Usage Logs & Access Records	2 years from date of activity	Security & fraud prevention
QR Submission Metadata & Timestamps	3 years from date of submission	Record integrity; legal reference
Billing & Transaction Records	8 years from transaction date	Statutory financial record-keeping
Support & Communication Records	3 years from last interaction	Dispute resolution; quality assurance

Upon expiry of the applicable retention period, data will be securely deleted or irreversibly anonymised. Anonymised and aggregated data (from which no individual or institution can be identified) may be retained indefinitely for research and analytical purposes.

## 9. Data Security

### 9.1 Technical & Organisational Measures

The Company implements appropriate technical and organisational security measures to protect data against unauthorised access, accidental loss, destruction, alteration, or disclosure. These measures include:

- Encryption of data in transit (using TLS/SSL protocols) and at rest;
- Role-based access controls and/or multi-factor authentication for platform administrators and analysts;
- Regular security vulnerability assessments and penetration testing;
- Incident response and breach notification procedures;
- Employee and contractor training on data protection and confidentiality obligations;
- Physical security measures at all facilities where data is processed.

### 9.2 Limitation of Security Guarantee

#### **⚠ Security Limitation Notice**

No data transmission over the internet or method of electronic storage is completely secure. While the Company employs industry-standard security measures, it cannot guarantee absolute security of data transmitted to or stored on the Platform. In the event of a security breach affecting personal data or Innovation Disclosure Data, the Company will notify the Institution without undue delay and in accordance

with applicable legal requirements, and will take all reasonable steps to mitigate the impact of such a breach.

## 10. Cookies & Platform Usage Tracking

The Platform may use cookies, session tokens, and similar tracking technologies to:

- Maintain login sessions and user preferences;
- Monitor platform performance and identify technical issues;
- Generate anonymised usage analytics to improve the Platform.

Essential cookies required for the Platform to function cannot be disabled. Non-essential analytical cookies may be managed through platform settings where available. The Company does not use third-party advertising or behavioural tracking cookies on the Platform.

## 11. Rights of Data Subjects

Subject to applicable law, Stakeholders and authorised representatives of the Institution have the following rights in respect of their personal data processed through the Platform:

- **Right of Access:** The right to request a copy of personal data held by the Company and information about how it is processed.
- **Right to Correction:** The right to request correction of inaccurate or incomplete personal data.
- **Right to Erasure:** The right to request deletion of personal data where it is no longer necessary for the purpose for which it was collected, subject to overriding legal obligations.
- **Right to Restrict Processing:** The right to request that the Company restrict processing of personal data in certain circumstances.
- **Right to Data Portability:** The right to receive personal data in a structured, commonly used, and machine-readable format, where technically feasible.
- **Right to Withdraw Consent:** Where processing is based on consent, the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before withdrawal.
- **Right to Grievance Redressal:** The right to lodge a complaint with the Company's Data Protection contact (see Section 15) or with the relevant data protection authority.

*Please note that certain rights may be limited or unavailable in respect of Innovation Disclosure Data where retention is required by law, for legitimate interests, or for the exercise or defence of legal claims. The Company will inform the relevant data subject of any applicable limitations when responding to a rights request.*

Requests to exercise any of the above rights should be submitted in writing to the Data Protection contact identified in Section 15. The Company will respond within thirty (30) days of receipt of a valid request.

## 12. Responsibilities of the Institution

The Institution, as a Data Fiduciary in respect of its Stakeholders, is responsible for:

1. Obtaining all necessary and legally valid consents from Stakeholders before submitting their personal data or Innovation Disclosure Data through the Platform;

2. Informing Stakeholders of the existence and contents of this Privacy Policy prior to their use of the Platform;
3. Ensuring that Stakeholders who are minors (under 18 years of age) do not submit data through the Platform without appropriate parental or guardian consent;
4. Promptly notifying the Company of any change in the status or rights of a Stakeholder (such as departure from the institution) that may require modification of data access or processing;
5. Maintaining its own records of Stakeholder consents and authorisations;
6. Not submitting to the Platform the confidential or proprietary data of third parties without appropriate authorisation.

## 13. Children's Data

---

The Platform is not designed for or directed at individuals under the age of 18. The Company does not knowingly collect personal data from minors. If the Institution becomes aware that a Stakeholder who has submitted data through the Platform is under 18, the Institution must immediately notify the Company. Upon receiving such notification, the Company will take appropriate steps to delete or restrict processing of such data.

## 14. Changes to This Privacy Policy

---

The Company reserves the right to update or amend this Privacy Policy at any time. Where changes are material, the Company will provide at least thirty (30) days' prior written notice to the Institution before the revised Policy takes effect. The Institution's continued use of the Platform following the effective date of any amendment constitutes acceptance of the revised Policy.

The version number and effective date of the current Policy will always be displayed on the Platform. Institutions are encouraged to review this Policy periodically.

## 15. Data Protection Contact & Grievance Officer

---

The Company has designated a Data Protection contact / Grievance Officer to handle data protection queries, rights requests, and complaints. All communications regarding this Privacy Policy or the Company's data processing practices should be directed to:

### **Grievance Officer / Data Protection Contact**

Karthick Manoharan  
Director  
EazelP LawTech Solutions, LLP.  
Email: [grievance@eazeip.com]  
Phone: [+91-9952166641]

*Response Time: Within 90 days of receipt of a written complaint or request.*

## 16. Governing Law

---

This Privacy Policy is governed by the laws of India. Any dispute arising from or in connection with this Privacy Policy shall be subject to the dispute resolution mechanism specified in the Platform's Terms & Conditions.

## 17. Acknowledgement

---

By accessing or using the Platform, the Institution and each Stakeholder confirm that they:

1. Have read and understood this Privacy Policy in its entirety;
2. Consent to the collection, processing, storage, and sharing of their data as described in this Policy;
3. Acknowledge that the Institution has fulfilled its responsibility to inform and obtain consent from all submitting Stakeholders;
4. Understand that Innovation Disclosure Data submitted through the Platform will be accessible to Patent Analysts and Platform administrators under strict confidentiality obligations.

— *End of Privacy Policy* —

Document Version 1.0 | Subject to periodic review. Always refer to the latest version on the Platform.

COPYRIGHT RESERVED – EAZEIP LAWTECH SOLUTIONS