PRIVACY POLICY (ePayCop)

Effective Date: 15/05/2025

This Privacy Policy explains how **XPECTRO SOLUTIONS (OPC) PRIVATE LIMITED ("Company", "we", "our", or "us")** collects, uses, discloses, and protects the personal information of users ("you", "your", or "user") who access or use the **ePayCop Mobile Application ("App")**. This Policy is in compliance with applicable Indian laws, including the Information Technology Act, 2000 and the rules made thereunder, and globally accepted privacy standards.

1. INFORMATION WE COLLECT

In the course of providing our services through the mobile application (**"App"**) and associated digital platforms, ***Xpectro Solutions (OPC) Private Limited*** may collect, store, process, and utilize certain categories of data and information from its users (hereinafter referred to as **"User", "you", or "your"**) as detailed hereinbelow. The collection, processing, retention, and usage of such data shall at all times be subject to applicable data protection laws, regulations, and the terms of this Privacy Policy.

1.1 Personal Information

For the purposes of this Privacy Policy, **Personal Information** shall mean any data or information that identifies or can be used to identify an individual User, either directly or indirectly. The Company, through the Application, collects and processes only the following categories of Personal Information, strictly for lawful, specific, and limited purposes connected with User registration, account management, and the provision of services:

I. **Full Name:** The name of the User as submitted during the account creation process.
II. **Mobile Number:** Collected for the purpose of account verification, authentication, service-related communications, and security alerts.
III. **Email Address:** Acquired for the issuance of registration confirmations, account-related correspondence, and service notifications.

The Company hereby affirms that it does not collect, process, or store any identity-related information, including but not limited to Aadhaar numbers, Permanent Account Numbers (PAN), dates of birth, residential or correspondence addresses, or any other official government-issued identification details.

Further, SMS data accessed through the Application's smishing detection feature is processed exclusively on the User's device for the purpose of identifying fraudulent or malicious content and is neither stored in the Company's databases nor transmitted to any external servers or third-party systems.

The Personal Information so collected is utilized solely for the performance of essential operational functions of the Application and shall not, under any circumstances, be sold, licensed, disclosed, or otherwise made available to any third-party entities for commercial marketing, promotional, or unrelated business purposes without the prior, explicit consent of the User, unless otherwise required by law.

1.2 Usage Data

Usage Data refers to non-personally identifiable information that is automatically collected by the Application and its associated systems during the User's interaction therewith. Such data may include, without limitation:

I. **Log Data and Metadata:** Records related to the User's access to and use of the Application, including session timestamps, features accessed, error logs, and diagnostic reports.
II. **Frequency and Duration of Use:** Analytical information regarding how often and for how long various features of the Application are utilized, for the purposes of operational optimization and service improvement.

III. **Device Information:** Technical details concerning the User's device, such as operating system type and version, device model, carrier information, and Application version number.

The collection and processing of Usage Data shall be conducted in compliance with applicable data protection laws and solely for legitimate operational, analytical, security, and service enhancement purposes. Usage Data shall not include personal identifiers beyond those necessary for these purposes.

1.3 Fraud Detection and Risk Management Data

To safeguard the integrity of digital transactions and mitigate risks associated with fraudulent, unlawful, or unauthorized activities, the Company may collect, monitor, and analyze limited categories of data strictly related to the features currently offered through the Application, including but not limited to:

I. **Scanned Links:** URLs and web addresses contained within SMS, email, or other messages accessed by the User via the Application, scanned solely for the identification of potential phishing, malware, or fraudulent content.
II. **Scam or Spam SMS:** Metadata and content analysis of unsolicited, scam-related, or potentially harmful text messages received by the User.

The collection, processing, and use of such data shall be undertaken exclusively for lawful, legitimate, and essential purposes directly connected with the functionality of the Application and shall be subject to appropriate technical and organizational security measures to prevent unauthorized access, disclosure, alteration, or destruction.

2. USE OF INFORMATION

2.1 Provision and Enhancement of Services

To facilitate, operate, manage, and enhance the functionalities, features, and user experience of the App, including but not limited to:

I. Enabling access to core services and functionalities provided through the App.
II. Customizing and optimizing the App's content, layout, and operational workflow based on User preferences and interaction history.
III. Diagnosing technical issues, conducting system audits, and implementing improvements to the App's performance, reliability, and security.

2.2 Fraud Detection, Prevention, and Risk Mitigation

To maintain digital security standards and protect Users against fraudulent or unauthorized activities, the Company may process specific categories of data strictly necessary for the operational functionality of the Application. This includes:

I. **Real-time assessment of SMS content and embedded URLs** to detect and flag malicious, fraudulent, or potentially harmful content.
II. **Issuance of security notifications or advisories to Users** in instances where a credible digital threat or smishing attempt is identified.

All data processing activities shall remain limited to purposes essential for the performance of the Application's existing security features.

2.3 User Notifications and Threat Alerts

To communicate directly with Users through in-app notifications, SMS, email, or other permitted communication channels in order to:

I. Notify Users of identified or potential cybersecurity threats, including phishing attempts, scam calls, smishing incidents, or other digital security risks.
II. Provide instructions, advisories, or remedial guidance in the event of exposure to such threats.
III. Ensure continuous awareness of evolving fraud trends and safety protocols.

2.4 Introduction of Enhanced Security Features

The Company reserves the right to introduce additional fraud prevention and digital security measures in future updates of the Application. Such enhancements shall be implemented in accordance with applicable legal requirements, and the processing of any new categories of personal data shall be subject to the User's prior

consent and notification through a revised Privacy Policy or applicable supplementary disclosure at the relevant time.

2.5 Communication, Support, and User Assistance

To facilitate prompt and effective communication with Users for the purposes of:

I. Addressing User queries, requests for support, complaints, or service-related feedback.
II. Sending administrative, transactional, or service-related communications, including policy updates, terms of use amendments, and security advisories.

2.6 Legal Compliance and Regulatory Obligations

To ensure compliance with applicable laws, rules, regulations, guidelines, and legal obligations imposed by statutory authorities, regulatory bodies, or competent courts of law, including but not limited to:

I. Maintenance of legally mandated records and audit trails.
II. Submission of information, reports, or disclosures as may be required under applicable law.
III. Assisting law enforcement or government agencies in the investigation, prosecution, or prevention of unlawful activities, subject to due legal process.

Note:
All use of personal data and sensitive personal information shall be strictly confined to the lawful purposes specified herein and shall be subject to the User's explicit or implied consent, wherever legally required. The Company undertakes to implement appropriate technical and organizational security measures to protect such data against unauthorized access, use, disclosure, or alteration.

3. LEGAL BASIS FOR PROCESSING PERSONAL DATA

The Company collects, processes, stores, and utilizes personal data and sensitive personal information in strict accordance with applicable data protection laws, including but not limited to the **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011**, and where applicable, the **General Data Protection Regulation (GDPR)**, in each case, as amended or re-enacted from time to time. The Company shall process personal data on the basis of the following legal grounds:

I. **the consent** of the Data Subject, which is obtained at the time of account creation, registration, or activation of specific functionalities within the App requiring the provision of personal data, with the understanding that such consent may be withdrawn by the Data Subject at any time, without affecting the lawfulness of processing prior to the withdrawal.
II. **legitimate interests** pursued by the Company, including but not limited to the prevention, detection, and mitigation of fraud (such as phishing, vishing, smishing, deepfake voice calls, and other forms of cyber fraud), ensuring the security and operational integrity of the App, and optimizing the User experience, provided that such legitimate interests are balanced against the fundamental rights and freedoms of the Data Subject, and subject to a legitimate interests assessment where required;
III. **the performance of a contract** between the Company and the Data Subject, or in order to take steps at the request of the Data Subject prior to entering into such a contract, including for the provision of services, administration of User accounts, and enforcement of the App's **Terms of Use** and **Privacy Policy**, with the understanding that the Data Subject's failure to provide necessary personal data may result in the inability to perform the contractual obligations; and
IV. **compliance with a legal obligation** to which the Company is subject, including but not limited to maintaining transaction records, submitting reports to regulatory bodies, fulfilling KYC (Know Your Customer) and AML (Anti-Money Laundering) requirements, and providing information to law enforcement agencies or courts in accordance with applicable laws, orders, or legal processes. In all instances, the Company shall ensure that personal data is processed lawfully, fairly, and transparently, and that appropriate technical and organizational measures are implemented to safeguard such data in accordance with applicable legal requirements.

4. DISCLOSURE OF INFORMATION

The Company hereby unequivocally affirms and declares that it does not, under any circumstances, engage in the sale, rental, licensing, or other form of commercial exploitation of the personal data, sensitive personal

information, or any other personally identifiable information (hereinafter collectively referred to as ***"Personal Data"***) of its Users (hereinafter referred to as ***"the Data Subject"***) to any third party for monetary consideration or otherwise. The confidentiality, privacy, and security of the Personal Data of our Users remains a matter of paramount importance and the Company undertakes to process, handle, and disclose such data strictly in accordance with applicable data protection laws and regulations, and, where applicable, the **General Data Protection Regulation (GDPR)** and any amendments or re-enactments thereof.

I. Notwithstanding the foregoing, the Company may, in the ordinary course of its legitimate business operations, disclose or transfer Personal Data to third parties under the following specific, limited, and lawfully permitted circumstances: To its **third-party service providers, consultants, affiliates, agents, contractors, or subcontractors** (collectively, "Service Providers"), who are engaged for the purpose of rendering essential services to or on behalf of the Company, including but not limited to cloud infrastructure hosting, data analytics, operational support, identity verification, fraud analysis, cyber security services, payment gateway facilitation, customer support, and IT infrastructure management. Such disclosures shall be strictly limited to the extent necessary for the provision of such services, and shall at all times be subject to legally binding contractual obligations, including but not limited to obligations of confidentiality, data protection, data security, and restrictions on secondary use of data, no less protective than those contained in this Privacy Policy and as required under applicable laws.

II. The Company may also disclose Personal Data to any **law enforcement authority, governmental or regulatory body, competent judicial or quasi-judicial authority, tribunal, or other statutory authority**, when such disclosure is, in the bona fide and reasonable opinion of the Company, necessary or mandated

(a) to comply with any applicable law, rule, regulation, order, judgment, decree, directive, or legally binding instruction, whether existing or forthcoming.

(b) to respond to lawful requests, subpoenas, summons, or investigative demands issued by a court of competent jurisdiction or any law enforcement or regulatory agency; or

(c) to discharge any obligation imposed upon the Company by any applicable regulatory framework.

III. Furthermore, the Company may disclose Personal Data where it is necessary to **protect, enforce, or defend the legitimate legal rights, proprietary interests, property, operations, or safety of the Company, its affiliates, employees, officers, directors, agents, or its Users**, including for the purposes of fraud prevention, risk assessment, investigation of unlawful activities, or safeguarding the security and integrity of the App and its associated systems and data.

IV. In the event that the Company undergoes any form of **corporate restructuring transaction**, whether by way of merger, acquisition, amalgamation, joint venture, assignment, sale of business, transfer of assets, or other form of corporate reorganization (collectively, "***Business Transaction***"), the Company reserves the right to transfer or assign the Personal Data of its Users as part of such Business Transaction to the relevant successor entity, purchaser, or counterparty, subject to such party's express undertaking to process and protect such Personal Data in accordance with privacy standards and security measures no less protective than those imposed under this Privacy Policy and applicable law.

In all instances of disclosure, the Company shall exercise commercially reasonable efforts to ensure that any third-party recipient of Personal Data is bound by appropriate confidentiality undertakings, contractual data protection obligations, and legally enforceable safeguards designed to ensure the lawful, fair, and secure processing of such data. The Company shall further undertake to notify Users, to the extent legally permissible, of any significant or material disclosure of Personal Data, particularly in instances involving a Business Transaction or governmental directive, where the disclosure materially affects the rights or interests of the Data Subject.

5. DATA SECURITY

We implement high technical and organizational security measures, including:

I. **End-to-End Encryption:**

All data transmissions between the User's device and the Company's servers are protected by industry-standard end-to-end encryption protocols to ensure confidentiality and prevent unauthorized interception, access, or tampering of data during transit.

II. **Role-Based Access Control (RBAC):**

Access to Data within the Company's systems and infrastructure is restricted and granted strictly on a need-to-know basis, in accordance with role-based access control mechanisms. Only authorized personnel with legitimate business purposes may access such data, subject to legally binding confidentiality and non-disclosure obligations.

III. **Secure Cloud Infrastructure:**

The Company operates its services on a secure, cloud-based infrastructure provided by reputed third-party service providers. Such infrastructure incorporates advanced security features, including multi-layered firewall protections, intrusion detection and prevention systems (IDPS), data redundancy, system hardening protocols, and periodic vulnerability assessments and penetration testing.

IV. **Real-Time Threat Monitoring and Incident Response:**

The Company employs continuous, real-time monitoring systems and automated threat detection tools to identify, log, and assess any suspicious activity, security vulnerabilities, or unauthorized access attempts. An incident response protocol is in place to promptly investigate, mitigate, and remediate any identified threats or breaches.

V. **Periodic Security Audits and Compliance Reviews:**

To ensure the sustained effectiveness, adequacy, and continual improvement of its data protection framework, the Company conducts periodic internal and external security audits, risk assessments, and compliance reviews, in line with applicable legal, regulatory, and contractual obligations.

VI. **Information Security Policies and Incident Management Protocol:**

The Company has adopted comprehensive, documented information security policies and data breach management procedures designed to provide clear guidelines for data protection, incident detection, investigation, containment, notification, and remediation in the event of any actual or suspected breach of Personal Data.

VII. **Third-Party Service Provider Obligations:**

All third-party service providers engaged by the Company for the processing or storage of Personal Data are required to comply with data protection obligations no less protective than those imposed upon the Company under this Privacy Policy and applicable law. Such service providers operate under binding contractual obligations relating to data security, confidentiality, and restricted secondary use of Personal Data.

VIII. **Limitation of Liability:**

While the Company undertakes to implement commercially reasonable and appropriate security measures as prescribed herein, it acknowledges that no security system is impenetrable. Accordingly, the Company disclaims liability for any unauthorized access, disclosure, alteration, or destruction of Personal Data caused by events beyond its reasonable control, provided that such disclaimer shall not apply to any breach attributable to the Company's gross negligence, willful misconduct, or breach of applicable data protection laws.

6. DATA RETENTION

Your personal data is retained:

I. **Retention for a Lawful, Specific, and Necessary Purpose:**

Personal Data shall be retained solely for such period as may be reasonably necessary to fulfill the legitimate, specified, and lawful purposes for which such data was originally collected, including but not limited to the provision of services, fraud detection and prevention, compliance with legal and regulatory obligations, dispute resolution, auditing, record maintenance, and enforcement of contractual rights and obligations.

II. **Compliance with Applicable Statutes and Regulations:**

The retention and preservation of Personal Data shall, at all times, be conducted in conformity with applicable statutory provisions, rules, regulations, and guidelines, 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, and, where applicable, the General Data Protection Regulation (GDPR), as amended or re-enacted from time to time, or any other relevant data protection legislations.

III. **Periodic Review and Assessment:**

The Company shall periodically undertake a systematic review and assessment of all retained Personal Data to determine its continued necessity, relevance, and compliance with applicable legal and operational requirements. Any Personal Data found to be obsolete, redundant, or no longer necessary for the legitimate purposes for which it was collected shall be subject to secure deletion, erasure, destruction, or irreversible anonymization, in accordance with applicable legal and industry standards.

IV. **Anonymization for Statistical and Analytical Use:**

Subject to the provisions of applicable data protection laws, the Company may, upon the expiry of the retention period or where such Personal Data ceases to be necessary, anonymize or pseudonymize such data for the purpose of conducting legitimate data analytics, system performance improvement, market research, and other lawful business purposes, ensuring that such data is rendered incapable of identifying any individual Data Subject.

V. **Retention for Legal Proceedings and Regulatory Compliance:**

Notwithstanding the general retention periods specified herein, the Company may retain Personal Data for such additional period as may be necessary to comply with legal obligations, enforce contractual rights, defend or establish legal claims, or respond to lawful requests from courts of law, governmental or regulatory authorities, law enforcement agencies, or in the context of any investigation, inquiry, or regulatory proceeding, to the extent permitted under applicable law.

VI. **Secure Disposal and Data Deletion Obligations:**

Upon the expiry of the prescribed retention period, or upon determination that the Personal Data is no longer required for the purposes for which it was collected, the Company shall ensure that such Personal Data is securely deleted, erased, destroyed, or irreversibly anonymized using appropriate technical and organizational measures consistent with prevailing industry practices and statutory data disposal standards. The Company shall maintain a verifiable record of such deletion or disposal actions undertaken, as required by applicable law.

7. YOUR RIGHTS

Subject to applicable laws, you have the right to:

Subject to applicable provisions of law, including but not limited to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, and, where applicable, the General Data Protection Regulation (GDPR), every individual whose personal data is collected and processed by the Company shall be entitled to exercise certain rights in respect of such personal data. The Data Subject shall have the right to obtain confirmation from the Company as to whether personal data concerning them is being processed and, where such processing is undertaken, to access such personal data, together with information relating to the categories of data processed, the purposes of processing, the recipients to whom such data has been disclosed, and the period for which the data is proposed to be retained.
Furthermore, the Data Subject shall have the right to request the rectification or correction of any inaccurate, incomplete, or outdated personal data maintained by the Company, without undue delay. Where processing is carried out on the basis of the Data Subject's consent, such consent may be withdrawn at any time by the Data Subject, provided that the withdrawal of consent shall not affect the legality of any processing previously undertaken based on such consent prior to its withdrawal. Additionally, subject to legal obligations and legitimate business purposes, the Data Subject may request the erasure or deletion of their personal data where it is no longer necessary for the purposes for which it was collected, or where consent has been withdrawn, or where the Data Subject objects to the processing and there exists no overriding legitimate reason for its continued processing.
The Data Subject shall also have the right to lodge a formal complaint before the competent data protection authority, regulatory authority, or supervisory authority having jurisdiction, in the event of any grievance or alleged non-compliance by the Company in relation to the processing or protection of personal data. Any such request or grievance by the Data Subject in relation to the aforementioned rights may be addressed in writing, stating clearly the nature of the request, to the Company at its designated official email address: ***service@xpectro-solutions.com***. The Company undertakes to acknowledge, address, and process such requests in accordance with applicable statutory provisions within the prescribed legal timelines.

8. CHILDREN'S PRIVACY

The Company expressly affirms that its digital services, including but not limited to its mobile application and associated platforms (hereinafter collectively referred to as **"the App"**), are not intended for use by individuals who are under the age of Thirteen 13 years. The Company does not knowingly or intentionally collect, solicit, process, store, or retain any personal data or sensitive personal information from any person who has not attained the age of majority as per applicable laws. In the event that it comes to the knowledge of the Company that personal data has been inadvertently collected from a minor without the verifiable consent of a lawful guardian or parent, the Company shall, upon becoming aware of the same, promptly delete, erase, or otherwise securely dispose of such data in accordance with applicable legal standards and data disposal protocols.
Further, the Company strongly advises and encourages parents, legal guardians, or persons having parental responsibility to supervise and monitor the online activities of minors and to ensure that no personal data is submitted to the App by individuals who have not attained the prescribed legal age for valid consent under applicable law. The Company disclaims any liability arising out of any personal data submitted by minors in contravention of this provision and reserves the right to restrict, terminate, or suspend access to the App in the event of a violation of this clause.

9. INTERNATIONAL DATA TRANSFERS

The Company acknowledges that, in the course of providing its services and in furtherance of its legitimate business operations, it may be necessary to transfer certain categories of personal data, including sensitive personal data or information, as defined under applicable law, to jurisdictions located outside the territorial boundaries of the Republic of India. The Company expressly affirms that any such cross-border transfer of personal data shall be carried out strictly in accordance with the provisions of the Information Technology Act, 2000, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, and any other applicable laws, rules, and regulations governing the protection and transfer of personal data.
In circumstances where the transfer of personal data is necessitated to countries or territories which may not offer an adequate level of data protection as recognized under Indian law, the Company undertakes to implement appropriate legal safeguards, including but not limited to the execution of standard contractual clauses, binding corporate rules, data transfer agreements, or other legally recognized mechanisms, to ensure that the personal data continues to receive a level of protection consistent with applicable legal requirements. The Company further affirms that all such international data transfers shall be conducted for lawful and necessary purposes,

including but not limited to the provision of services, fraud detection, cloud hosting, analytics, and compliance with contractual obligations, and that reasonable security practices and procedures shall be adopted to safeguard the integrity and confidentiality of such data at all times.

10. THIRD-PARTY LINKS AND SERVICES

I. **Inclusion of Third-Party Links:**

The App may contain hyperlinks, references, or connections to external third-party websites, services, or application programming interfaces (APIs), including but not limited to services for payment processing, verification, or other functionalities (hereinafter referred to as ***"Third-Party Services"***).

II. **Non-Liability for Third-Party Privacy Practices:**

The Company expressly disclaims any responsibility or liability for the privacy practices, policies, or actions of such Third-Party Services, including the manner in which personal data may be collected, processed, or stored by such third parties.

III. **Review of Third-Party Policies:**

Users are strongly encouraged to review the privacy policies, terms of service, and any other legal documents of the Third-Party Services accessed via links within the App. The Company shall not be liable for any actions, omissions, or consequences resulting from the use of any third-party websites or services.

11. CONSENT AND CHANGES TO POLICY

I. **Consent to Data Collection and Use:**

By accessing, using, or interacting with the App, the User hereby provides explicit consent to the collection, processing, and use of their personal data as described in this Privacy Policy. The User acknowledges and agrees to the terms and conditions set forth herein with respect to their personal data.

II. **Right to Amend the Privacy Policy:**

The Company reserves the right, at its sole discretion, to modify, amend, update, or otherwise alter this Privacy Policy at any time and without prior notice, in order to reflect changes in legal, regulatory, or operational requirements or for any other purpose deemed necessary by the Company.

III. **Acceptance of Changes:**

The continued use of the App following any such amendments, modifications, or updates to the Privacy Policy shall be deemed as the User's acceptance of such changes. The User is encouraged to review this Privacy Policy periodically to remain informed of any updates or modifications.

12. GRIEVANCE REDRESSAL OFFICER

I. **Appointment and Responsibility:**

In compliance with Rule 5(9) of the **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011**, the Company has appointed a Grievance Redressal Officer to address complaints related to personal data processing and privacy concerns.

II. **Contact Information:**

Email: service@xpectro-solutions.com
Address: 4th Floor, Workpod India, Plot 93, Sector 44, Gurugram, Haryana 122003, India
Response Time:
The Grievance Redressal Officer will acknowledge receipt of complaints within 7(Seven) business days and work to resolve them appropriately, in accordance with applicable privacy laws.

13. FUTURE USE OF AI-BASED FEATURES

The Company may, in future updates or enhanced versions of the Application, incorporate advanced fraud detection, security, or risk mitigation functionalities powered by artificial intelligence (AI) and other emerging technologies.
Any collection, processing, or use of additional categories of personal data beyond those currently specified in this Privacy Policy shall be carried out strictly in compliance with applicable laws and regulations and only upon obtaining the User's prior, explicit, and informed consent for such specific purposes.
All such future data processing activities, if introduced, shall be governed by a duly updated Privacy Policy or a supplementary privacy notice, which shall be communicated to the User in advance and shall expressly detail the nature, scope, purpose, and legal basis of the proposed data collection and processing.

14. RESTRICTIONS ON MISUSE

By using the App, you agree not to misuse or abuse the services provided therein, including but not limited to attempting to bypass or circumvent the App's fraud detection systems, security measures, or other protective features implemented by the Company. Any unlawful or unauthorized activity, such as engaging in fraudulent actions, attempting to gain unauthorized access, or interfering with the integrity of the App's fraud prevention mechanisms, shall be considered a breach of the terms and conditions of use. In the event of any misuse or illegal activity, the Company reserves the right to immediately terminate access to the App and take appropriate legal action, including reporting the incident to relevant law enforcement authorities as necessary, in accordance with applicable laws and regulations.

15. COMPLIANCE WITH INDIAN LAW

This Privacy Policy, along with all matters connected with or incidental to it, shall be governed by and construed in strict accordance with the laws for the time being in force in the Republic of India. The Parties expressly agree that any disputes, claims, or legal proceedings arising out of or in connection with this Privacy Policy, including its interpretation, application, or enforcement, shall be subject to the exclusive jurisdiction of the competent courts situated at Gurugram, Haryana, India. By accessing and using the App, the User expressly submits to the jurisdiction of such courts and waives any objection to such jurisdiction or venue on any grounds, including the grounds of forum non convenience.

16. CONTACT US

In the event that you, the User, have any queries, concerns, grievances, or require any clarifications in relation to this Privacy Policy or the manner in which your personal data is collected, processed, stored, or otherwise handled by the Company, you may contact us using the details provided herein. All such communications should be directed to **Xpectro Solutions (OPC) Private Limited** through the following modes of correspondence:

- **Email:** service@xpectro-solutions.com
- **Website:** www.xpectro-solutions.com

The Company shall endeavor to address and resolve any concerns or queries received at the earliest, in accordance with the applicable legal provisions and within the timelines prescribed under the relevant data protection laws.

The Company hereby reaffirms its commitment to maintaining the highest standards of privacy, confidentiality, and data security in relation to the personal data collected, processed, and retained through the use of the App. Users are expressly advised to periodically review the terms of this Privacy Policy in order to remain apprised of

any amendments, modifications, or updates which may be effected by the Company from time to time, to ensure continued compliance with prevailing legal and regulatory requirements.

The Company expressly reserves the right to amend, revise, or modify this Privacy Policy at its sole and absolute discretion, without prior notice, and such revised policy shall be deemed effective and binding from the date of its publication on the official platform or website of the Company. Continued access to and use of the App by the User subsequent to such revisions shall constitute the User's deemed acknowledgment, acceptance, and agreement to be bound by the updated provisions of this Privacy Policy.

The Company assures all users that it remains steadfastly committed to protecting personal data against unauthorized access, disclosure, or misuse and to ensuring that all data processing activities are undertaken in accordance with the applicable laws of India and relevant international best practices, wherever applicable.