PRIVACY POLICY (APIs)

Effective Date: 15/12/2025

1. INTRODUCTION

This API Privacy Policy governs the access to and use of the application programming interfaces (APIs) provided by **Xpectro Solutions (OPC) Private Limited** ("Company", "we", "us"). This policy is an extension of our general Privacy Policy and Terms of Service. By integrating or using our APIs, you ("User", "Developer", "Customer") consent to the practices described herein.

2. SCOPE AND DEFINITIONS

This policy applies specifically to data collected through our API endpoints, developer portals, and sandbox environments.

- **"API Client Data"** refers to information about you, the developer or business customer, required to manage your account and billing.
- **"Input Data"** refers to the data you send to our APIs for processing (e.g., URLs for smishing analysis, voice samples, or phone numbers).
- **"Technical Usage Data"** refers to metadata generated by your interaction with our services (e.g., API call logs, timestamps, IP addresses).

3. INFORMATION WE COLLECT

3.1. API Client Account Data

To provide access to the API, we collect "Personal Data" and "Sensitive Personal Data" relating to the account holder. This includes:

- **Identity Data:** Name, organization name, and email address for API key issuance.
- **Financial Data:** Bank account or credit card details processed by our payment gateway partners for billing subscription fees.

3.2. API Input Data (Payloads)

When you make a request to our APIs (e.g., the ePayCop Smishing Detection API), we receive the data included in the request payload.

- **Content:** This may include URLs, SMS text content, phone numbers, or other digital artifacts required to perform the detection service.
- **Data Minimization:** You agree to only send the specific data required for the API to function and to refrain from sending unrelated Sensitive Personal Data unless explicitly authorized.

3.3. Technical and Log Data

Our systems automatically record "Technical Information" regarding your API usage. This includes:

- **Device & Network:** Internet Protocol (IP) address, operating system, and client identifiers.
- **Usage Metrics:** Date and time of requests, latency, endpoint success/failure rates, and clickstream data.

4. HOW WE USE YOUR DATA

We use the collected information for "Legitimate Purposes" permitted under applicable laws:

- **Service Delivery:** To authenticate your API keys, process your Input Data (e.g., scanning a URL for threats), and return the requested results.
- **Billing and Administration:** To manage your subscription, send invoices, and communicate changes to API versions or policies.
- **Product Improvement & Research:** We use anonymized and aggregated Input Data and Usage Data to improve our detection algorithms (e.g., training our AI models to better recognize smishing patterns) and for academic research.
- **Security & Fraud Prevention:** To detect anomalous traffic, prevent denial-of-service attacks, and identify unauthorized use of API credentials.

5. DATA STORAGE AND RETENTION

Location: Data is primarily stored in electronic form on secure servers. We may store or process data in countries outside of India, ensuring compliance with applicable laws and reasonable security standards.

Retention Period:

- **Account Data:** Retained as long as your account is active or as needed to comply with legal obligations.
- **Input Data:** We may retain anonymized Input Data for research and product improvement purposes indefinitely, provided it does not identify any natural person.

- **Deletion:** Upon cancellation of your account, we are not obligated to retain your data, though legal records may be kept for the maximum period permitted by law.

6. DATA SHARING AND DISCLOSURE

We do not sell your data. We share information only in the following scenarios:

- **Service Providers:** We share limited data with third-party vendors (e.g., cloud hosting providers, payment processors) strictly to render the Services.
- **Legal Compliance:** We may disclose information to law enforcement or government authorities if required by legal, judicial, or quasi-judicial processes.
- **Business Transfers:** In the event of a merger or acquisition, collected information may be transferred to the new entity.

7. SECURITY

We employ industry-standard physical, managerial, and technical safeguards to protect your data.

- **Encryption:** We use secure servers and encryption for data transmission.
- **Disclaimer:** While we strive for security, no internet transmission is 100% secure. We cannot guarantee absolute security of data transmitted to our APIs.

8. YOUR RIGHTS

Subject to applicable laws, you have the right to:

- **Access and Update:** Edit your account information via the developer portal or by contacting us.
- **Object/Restrict:** Request restrictions on the processing of your Personal Information.
- **Portability:** Request a transfer of your Personal Information in a machine-readable format. To exercise these rights, email us at service@xpectro-solutions.com .

9. CONTACT AND GRIEVANCE REDRESSAL

In compliance with the Information Technology Act, 2000, we address grievances within 15 days of receipt.

- **Contact Email:** service@xpectro-solutions.com
- **Process:** Please provide detailed information regarding your concern or grievance to allow us to assist you effectively.