Privacy and Data Protection Policy for Anti-Scam Network

Effective Date: April 14, 2025

Version: 1.2

1. Introduction and Purpose

This comprehensive privacy policy governs our anti-scam Discord bot's data handling practices. Our primary mission is to protect Discord communities from fraudulent activities through responsible information sharing and automated protection measures.

2. Legal Basis for Processing

We process data under the following legal bases:

- Legitimate interest in preventing fraud and protecting users
- Explicit consent from server administrators
- Legal obligations for crime prevention

3. Data Collection and Processing

We collect and process the following essential information:

- Primary Identifiers:
  - Discord User IDs of confirmed scammers
  - Server IDs where incidents occurred
  - Timestamp and duration of incidents

- Evidence Records:
  - Screenshots of scam attempts
  - Chat logs related to scam incidents

Transaction records (when applicable)

All data stored was submitted with the consent of the user uploading the material.

4. Enhanced Security Measures

Your data is protected by:

- Multi-factor authentication for administrative access
- Real-time monitoring
- Automated backup systems

5. Data Sharing Protocol

Authorized Recipients:

Verified server owners (through secure API)

Trusted partner networks (with data processing agreements)

Law enforcement (with valid legal requests)

Sharing Restrictions:

End-to-end encrypted transmission

Rate-limited API access

Audit logging of all data access

6. Enhanced User Rights

We guarantee expanded user rights:

Access to personal data within 72 hours of request

Right to appeal with new evidence (14-day window)

Data portability in machine-readable format

Right to erasure after verification

7. Sophisticated Data Retention

Active Records:

- Confirmed scam incidents: Permanent
- Appeal documentation: 6 months post-resolution
- Chat logs: Permanent

- Archived Records:
  - Statistical data: Permanent
  - Pattern analysis data: Permanent

8. Incident Response

Our incident response framework includes:

- 24/7 automated monitoring
- 72-hour maximum response time for appeals
- Regular staff training

9. Compliance and Oversight

We maintain compliance through:

- Compliance with GDPR and CCPA requirements
- Transparent reporting of enforcement actions
- Annual privacy policy reviews

> Warning: Submitting false scam reports is a serious violation. Verified false reports will result in immediate network-wide ban and potential legal consequences.

This policy is regularly updated to reflect new security measures and community protection standards.