

Privacy Policy

Effective Date: 1 June 2026 | **Last Updated:** 1 June 2026

Important Notice

This Privacy Policy (“Policy”) explains how we collect, use, store, and protect information when you use our mobile application (the “App”), an AI-powered virtual cat experience available on Google Play.

Read with the Terms of Service. This Policy must be read together with our Terms of Service, which set out additional terms, disclaimers, limitations of liability, dispute resolution and governing law. In the event of any conflict between this Policy and the Terms of Service in respect of liability, dispute resolution, or governing law, the Terms of Service shall prevail.

Age Restriction. The App is intended exclusively for users aged 18 and over. If you are under 18, you must not download, install, or use the App. Age verification is based on (i) your self-declaration upon account creation and (ii) the Google Play age-rating mechanism. We do not perform additional age verification and assume no responsibility for data submitted by persons who misrepresent their age.

Geographic Availability. The App is made available primarily in the Philippines and other markets outside the European Union and European Economic Area. Distribution of the App in the EU/EEA is restricted through Google Play country-availability settings. Notwithstanding such restriction, the Developer is established in the Netherlands and therefore the EU General Data Protection Regulation (Regulation (EU) 2016/679, “GDPR”) applies to our processing activities pursuant to Article 3(1) GDPR. We comply with GDPR in respect of all personal data we process, regardless of user location.

1. Who We Are (Data Controller)

The Data Controller for the personal data processed in connection with the App is:

- **Name:** Ilia Chasovnikov
- **Status:** individual app developer (natural person) acting as Data Controller
- **Country of establishment:** the Netherlands
- **Contact email:** support@toonlabs.co

No corporate legal entity has been established. Where mandatory law permits an individual controller to communicate via electronic means only, communications shall be addressed to the contact email above.

2. Information We Collect

Consistent with our Google Play store disclosures, we may collect the following categories of data. Collection of specific items depends on your interactions with the App and the features you choose to use.

2.1 Personal Information

- **Name** — voluntarily provided for personalization.
- **Email address** — used for account identification and support communications.
- **User identifiers** — internal IDs we generate to recognize your account, device, and session.

- **Other personal information** — any additional details you choose to provide voluntarily.

2.2 Photos and Videos

- **Photos** — images you upload, capture, or share with the AI cat.
- **Videos** — video content you upload or share within the App.

2.3 Audio

- **Audio recordings, including voice messages** — voice input you send to the AI cat.

2.4 App Information and Performance

- **Crash logs** — automatic reports generated when the App malfunctions.
- **Diagnostics** — performance metrics such as load times, battery usage, and errors.
- **Other app performance data** — technical telemetry necessary to operate the App.

2.5 App Activity

- **In-app actions** — interactions (taps, screens viewed, features used).
- **Other user-generated content** — text and other content you create or input.

2.6 Device and Advertising Identifiers

Our analytics and crash-reporting providers (Firebase, Amplitude) may collect device-level identifiers, including the Google Advertising ID (GAID) on Android devices, for the purpose of de-duplicating analytics events and crash reports. We do not use these identifiers for advertising, targeting, or sale to third parties. You may reset or limit your advertising identifier at any time through your device settings (Android: Settings → Google → Ads).

2.7 Push Notification Tokens

If you enable push notifications, we process a device-level push notification token (issued by Firebase Cloud Messaging) for the sole purpose of delivering notifications related to the App. You may disable push notifications at any time through your device system settings, in which case we cease using the token for delivery.

2.8 Nature of Voice, Photo and Video Data

We process voice recordings, photographs and videos solely as conversational input for the AI cat to generate a response. We do not perform facial recognition, voiceprint identification, biometric template extraction, or any biometric identification of any individual. The content is not used to uniquely identify a natural person within the meaning of Article 4(14) GDPR and does not constitute biometric data for identification purposes. Notwithstanding the foregoing, we treat such content as sensitive in practice and process it only on the basis of your explicit consent (see Section 4).

2.9 Your Responsibility for Submitted Content

You are solely responsible for any data, content, photos, videos, audio, or text you submit to the App. You represent and warrant that you have all necessary rights to submit such content and that doing so does not violate any third party's rights or any applicable law. You agree to indemnify and hold us harmless from any claims arising out of content you submit.

We do not collect: financial information, payment data, precise geolocation, contacts, calendar, SMS, health or fitness data, web browsing history, or messages from other apps. The App does not contain in-app purchases, subscriptions, or any payment functionality.

3. How We Use Your Data

We use collected data for the following purposes:

- To operate the AI cat (process inputs and generate AI responses).
- To maintain and improve App stability and performance.
- To conduct internal product analytics.
- To respond to support requests.
- To deliver push notifications, where you have enabled them.
- To enforce our Terms of Service and prevent abuse, fraud, and unlawful use.
- To comply with legal obligations and respond to lawful requests from authorities.

We do not sell personal data, do not share it with advertisers, and do not use your content to train AI models.

4. Legal Basis for Processing

Under GDPR, we rely on the following legal bases:

- **Performance of a contract (Article 6(1)(b))** — for processing necessary to deliver the App and the AI cat functionality you requested.
- **Legitimate interests (Article 6(1)(f))** — for product analytics, debugging, fraud prevention, security and product improvement, balanced against your rights and freedoms.
- **Consent (Article 6(1)(a))** — for the processing of photos, videos, audio recordings and voice messages that you voluntarily submit to the App; for push notifications; and where otherwise required by law. You may withdraw consent at any time, in which case we cease the relevant processing (subject to processing already completed in reliance on consent and to retention required by law). Withdrawal of consent for content processing may be exercised by deleting your account or by requesting deletion under Section 8.
- **Legal obligation (Article 6(1)(c))** — where processing is necessary to comply with a legal obligation to which we are subject.

To the extent any photo, video or audio content you submit could, in a given context, be considered “special categories of personal data” under Article 9 GDPR (for example, where you voluntarily reveal information about your health, ethnic origin, religious beliefs, sexual orientation or similar matters), we process such data solely on the basis of your explicit consent under Article 9(2)(a) GDPR, which you provide by knowingly submitting such content to the App. You should not submit content revealing such matters unless you wish such processing to occur.

5. Third-Party Service Providers

We rely on third-party processors to operate the App. These providers act under their own privacy policies and terms. We exercise reasonable care in selecting them but are not responsible or liable for their acts, omissions, security incidents, or changes to their services. Your data, when processed by these providers, is subject to their respective policies.

Provider	Purpose	Location	Privacy Policy
Amazon Web Services (AWS)	Cloud hosting and storage	United States (us-east-1, Virginia)	aws.amazon.com/privacy
Google Firebase / FCM	Crash reporting, diagnostics, push notifications	Google data centers (global)	firebase.google.com/support/privacy
Amplitude	Product analytics	United States	amplitude.com/privacy
OpenAI (GPT family models)	AI response generation	United States	openai.com/policies/privacy-policy

OpenAI processing. We use language models from OpenAI's GPT family for AI response generation. The specific model in use may be updated from time to time without amendment to this Policy. Content of your inputs (text messages, transcribed voice and descriptions of submitted media) is transmitted to the OpenAI API for one-time inference. Per OpenAI's API data usage policy, API inputs are not used to train OpenAI models. OpenAI may retain inputs for a limited period for abuse-monitoring purposes, after which they are deleted in accordance with OpenAI's policies. We have no control over OpenAI's internal processing, retention or security and disclaim liability for any acts or omissions of OpenAI to the maximum extent permitted by law.

6. International Data Transfers

Your data is stored and processed primarily in the United States (AWS us-east-1, Virginia, and OpenAI infrastructure). By using the App you acknowledge and consent to your data being transferred to, and processed in, the United States, which may have data protection laws different from those of your country of residence.

Transfers from the Netherlands (where the Controller is established) to the United States are made on the basis of (i) the EU-US Data Privacy Framework where the recipient is certified, and/or (ii) Standard Contractual Clauses (SCCs) approved by the European Commission. We rely on the standard data-processing terms offered by AWS, Google, Amplitude and OpenAI, each of which incorporates SCCs for international transfers.

7. Data Retention

We retain data for as long as reasonably necessary for the purposes set out in this Policy. Indicative retention periods (not strict deadlines):

- **Active accounts** — personal data is retained while your account is active.
- **Inactive accounts** — we use reasonable efforts to schedule for deletion personal information of accounts that remain inactive for at least two (2) consecutive years.
- **Crash logs and diagnostics** — typically retained for up to 90 days.
- **Aggregated and anonymized data** — may be retained indefinitely as it does not identify you.

We may also retain data for longer where required for legal, regulatory, tax, accounting, dispute-resolution or fraud-prevention purposes.

8. Your Rights and How to Exercise Them

Under GDPR (and, where applicable to users located in the Philippines, the Data Privacy Act of 2012, Republic Act No. 10173), you have the following rights:

- **Right of access (Article 15)** — obtain confirmation of whether we process your data and a copy of such data.
- **Right to rectification (Article 16)** — request correction of inaccurate or incomplete data.
- **Right to erasure (Article 17)** — request deletion of your personal data.
- **Right to restriction of processing (Article 18)** — request that we limit how we use your data in certain circumstances.
- **Right to data portability (Article 20)** — receive your data in a structured, commonly used, machine-readable format and have it transmitted to another controller where technically feasible.
- **Right to object (Article 21)** — object to processing based on legitimate interests.
- **Right to withdraw consent (Article 7(3))** — at any time where processing is based on consent.
- **Right to lodge a complaint (Article 77)** — with a competent data protection authority, including the Dutch Data Protection Authority (Autoriteit Persoonsgegevens, autoriteitpersoonsgegevens.nl).

How to Exercise Any of Your Rights

To exercise any of the rights listed above, send a written request to **support@toonlabs.co** from the email address linked to your account. Please include:

- Your account email and any user identifier visible in the App.
- A clear statement specifying which right you wish to exercise (access, rectification, erasure, restriction, portability, objection, or withdrawal of consent).
- Any further information reasonably necessary to verify your identity.

We will use reasonable efforts to respond to verified requests within thirty (30) calendar days of receipt. Where requests are complex or volumes are high, we may extend this period by up to a further sixty (60) days and will notify you of any such extension. We may refuse or charge a reasonable fee for requests that are manifestly unfounded, excessive or repetitive, or where we cannot verify your identity.

Specific Procedure for Data Deletion

Upon a verified deletion request, we will use reasonable efforts to delete the following:

- Personal information (name, email, user identifiers, and other personal details).
- Photos you uploaded.
- Videos you uploaded.
- Audio recordings and voice messages.

The following will be anonymized rather than deleted:

- In-app activity records (taps, screens viewed, features used) — retained in anonymized, non-identifiable form for product analytics.

Some data may be retained beyond a deletion request where required by law, for the establishment, exercise or defence of legal claims, or where deletion is technically infeasible without disproportionate effort (in which case the data will be isolated from further active use).

9. Automated Decision-Making and Profiling

We do not use your personal data to make decisions, based solely on automated processing (including profiling), that produce legal effects concerning you or similarly significantly affect you within the meaning of Article 22 GDPR. AI responses generated by the App are conversational outputs only and do not constitute decisions of legal or similar significance.

10. Security; No Warranty of Security

We apply technical and organizational measures consistent with industry practice, including:

- Encryption in transit (TLS) between your device, our servers, and third-party processors.
- Encryption at rest for stored data on AWS.
- Access controls on a need-to-know basis.
- Periodic reviews of our infrastructure and dependencies.

No system is fully secure. Despite reasonable measures, no method of transmission over the Internet or method of electronic storage is completely secure. We do not warrant or guarantee the security of any data and, to the maximum extent permitted by law, we expressly disclaim all liability for any unauthorized access, loss, alteration, or disclosure of data, including but not limited to losses caused by third parties, hacking, social engineering, malware, or events outside our reasonable control (force majeure).

11. Personal Data Breach Notification

In the event of a personal data breach (within the meaning of Article 4(12) GDPR) that is likely to result in a risk to your rights and freedoms, we will notify the competent supervisory authority (the Dutch Data Protection Authority, Autoriteit Persoonsgegevens) without undue delay and, where feasible, not later than 72 hours after having become aware of the breach, in accordance with Article 33 GDPR. Where the breach is likely to result in a high risk to your rights and freedoms, we will also notify affected users without undue delay in accordance with Article 34 GDPR, unless an exception under Article 34(3) applies.

12. Children's Privacy

The App is intended for users aged 18 and over only. We do not knowingly collect personal data from anyone under 18. If we become aware that we have inadvertently collected personal information from a person under 18, we will use reasonable efforts to delete it promptly. If you believe a child has provided us with information, please contact support@toonlabs.co.

13. Artificial Intelligence Notice and Disclaimer

The App uses language models from OpenAI's GPT family, provided by an independent third party and subject to change without notice. You acknowledge that:

- **AI outputs are generated and may be inaccurate.** They are not, and shall not be considered, professional advice (medical, legal, financial, psychological or otherwise).
- **AI may produce unexpected or unsafe outputs.** You agree not to rely on AI outputs for any decision having material consequences.

- **Do not submit sensitive information** (financial credentials, government IDs, health data) to the AI chat.
- **We have no control over the underlying AI model** and disclaim all liability for outputs, errors, omissions, or harm caused by AI responses to the maximum extent permitted by law.
- **One-shot processing.** Your inputs are sent to OpenAI for a single inference operation and are not used to train AI models.

14. Changes to This Policy

We may modify this Policy from time to time to reflect changes in our practices, technology, partners or legal obligations. Where reasonably practicable, we will provide notice of material changes via the App or by email. The current version is identified by its Effective Date. Your continued use of the App after the Effective Date of a revised Policy constitutes your acceptance of the revised Policy.

15. Force Majeure

We are not liable for any failure or delay in performance of this Policy or applicable obligations resulting from events beyond our reasonable control, including acts of God, natural disasters, war, terrorism, civil unrest, government action, pandemics, labor disputes, internet or telecommunications failures, cyberattacks, third-party service outages, or denial-of-service events. This Section does not exclude or limit any liability that cannot be excluded or limited under applicable law.

16. Governing Law

This Policy is governed by, and construed in accordance with, the laws of the Netherlands, without regard to its conflict-of-laws provisions. Dispute resolution provisions, including mandatory arbitration and class-action waivers, are set out in the Terms of Service.

17. Severability

If any provision of this Policy is held to be invalid, illegal or unenforceable in any jurisdiction, the remaining provisions remain in full force and effect, and the invalid provision shall be modified to the minimum extent necessary to make it enforceable while preserving its original intent.

18. Contact

For any questions, concerns, requests, or to exercise your privacy rights:

Data Controller: Ilia Chasovnikov, the Netherlands

Email: support@toonlabs.co

Where a Russian-language version of this Policy is provided, it is for convenience only. The English version is the binding text and prevails in case of any inconsistency.