

Privacy Policy — Linkoglot

Version: **v1.0.0**

Effective date: **2026-06-07**

Last updated: **2026-06-07**

Introduction

This Privacy Policy explains how Linkoglot ("Linkoglot", "we", "us", "our") collects, uses, discloses, retains and protects personal data in connection with the Linkoglot web and mobile application (the "App"). This Policy is drafted to comply with Regulation (EU) 2016/679 (GDPR/RODO) and applicable Polish law.

If you have questions about this Policy or wish to exercise your rights, contact us at contact@linkoglot.eu or at the postal address below.

Scope and principles

We apply the principles of lawfulness, fairness, transparency, data minimisation, purpose limitation, accuracy, storage limitation, integrity and confidentiality. We collect only personal data necessary to provide the App's services, meet legal obligations, and protect legitimate interests related to security and fraud prevention.

Account deletion

You can delete your account in the App settings. You can also request account deletion through <https://www.linkoglot.eu/en/DeleteAccount>. When you delete your account, we delete or anonymize the personal data associated with that account, except where we must retain certain data for security, fraud prevention, or legal compliance reasons.

Categories of data we collect

Linkoglot collects and processes the following categories of personal data:

- **Personal info:** name, email address, profile picture, and other data received from third-party authentication providers such as Google LLC and Apple Inc. Passwords are securely processed by our authentication service and are not readable by us.
- **Purchase history:** information about subscriptions and in-app purchases, including product identifiers, entitlement status, purchase dates, renewal dates, and transaction references used to provide and manage paid features.
- **Photos:** images uploaded by users for AI-powered analysis and flashcard generation. Images are processed only to provide the requested feature. We do not store uploaded images after processing is completed, and we do not use uploaded images for AI model training or improvement.
- **Messages:** text content you submit through in-app forms, including bug reports, support requests, and AI prompt inputs or generation requests. This data is processed to provide the requested functionality, respond to support requests, maintain user-submitted records where applicable, troubleshoot errors, prevent abuse, and secure the App. We do not use Messages for third-party AI model training.
- **App activity:** information about user interactions within the App, including flashcards created, study sessions, XP progression, streaks, and other in-app activity related to learning features.
- **App info and performance:** App version, build number, device model, crash reports, loading times, and technical diagnostics required to operate, maintain, and secure the App.
- **Usage analytics:** App interaction metrics such as feature usage, navigation patterns, session behavior, and engagement analytics used to improve features and user experience.
- **Device or other IDs:** push notification tokens, authentication identifiers, platform identifiers, and other identifiers necessary for authentication, security, fraud prevention, and service functionality.

Data type	Collection purpose	Processors	Required	Processed ephemerally	Retention
Personal info	✓ App functionality ✓ Account management	✓ App functionality ✓ Account management	Yes ▾	No ▾	Until account deletion
Purchase history	✓ App functionality ✓ Analytics ✓ Fraud prevention, security and compliance ✓ Account management	✓ App functionality ✓ Analytics	Yes ▾	No ▾	Until account deletion, unless required for legal obligations
Photos	✓ App functionality	✓ App functionality	No ▾	Yes ▾	Deleted immediately after processing
Messages	✓ App functionality ✓ Analytics ✓ Developer communications	✓ App functionality ✓ Analytics ✓ Developer communications	No ▾	No ▾	Until account deletion
App activity	✓ App functionality ✓ Analytics ✓ Developer communications	✓ App functionality ✓ Analytics ✓ Developer communications	Yes ▾	No ▾	Until account deletion
App info and performance	✓ Analytics	✓ Analytics	Yes ▾	No ▾	Retention varies by provider (Sentry)
Usage analytics	✓ Analytics	✓ Analytics	No ▾	No ▾	Retention varies by provider (Vexo)
Device or other IDs	✓ App functionality ✓ Analytics ✓ Fraud prevention, security and compliance ✓ Account management ✓ Developer communications	✓ App functionality ✓ Analytics ✓ Fraud prevention, security and compliance ✓ Account management ✓ Developer communications	Yes ▾	No ▾	Until account deletion

Legal bases for processing

We process personal data on one or more of the following lawful bases:

- **Performance of a contract (Article 6(1)(b) GDPR):** account creation, authentication, subscription management via Apple, Google, and RevenueCat, provision of core App functionality, paid features, AI Credits, AI-powered text generation, AI-powered image/photo analysis, AI-powered text-to-speech generation, flashcard generation, purchase-related records, and service-related communications necessary to administer your account, subscription, purchases, and use of the App.
- **Consent (Article 6(1)(a) GDPR):** We rely on your consent for:
 - sending marketing, promotional, engagement-related, and optional product communications by email, push notification, in-app message, or other available communication channels, where such consent is required by law;
 - collecting analytics data (usage analytics and app behavior tracking).Consent is freely given, specific, informed, and can be withdrawn at any time through in-app settings or device settings. Withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.
- **Legitimate interests (Article 6(1)(f) GDPR):** improving app performance and stability, crash reporting, troubleshooting, fraud prevention, abuse detection, security, service integrity, and sending important non-marketing service notices where necessary to operate, protect, or administer the App, provided these interests are not overridden by your rights and freedoms.
- **Legal obligation (Article 6(1)(c) GDPR):** retention of records required for compliance with applicable laws, including subscription and transaction records (via Apple, Google, and RevenueCat where applicable) and basic accounting or tax obligations where required.

AI processing and model training

We use third-party AI service providers to process user-submitted text, uploaded images, and generated outputs only to provide the requested App functionality, such as AI-powered content generation, image/photo analysis, flashcard generation, and text-to-speech generation.

We do not permit AI service providers to use user-submitted prompts, uploaded photos/images, or generated outputs to train, improve, or evaluate their models where we have control over such settings. We configure OpenRouter requests with provider data collection disabled and do not use free AI models or provider routes that may use user data for model training.

We do not enable optional OpenAI data-sharing, model-improvement, evaluation, fine-tuning, or inputs/outputs sharing settings for user data.

AI service provider metadata

AI service providers may process and retain limited operational metadata necessary to provide, secure, bill, monitor, debug, and improve the reliability of their services. This may include metadata such as request timestamps, model used, token counts, latency, routing information, request identifiers, cost or billing information, error logs, and similar technical information.

This operational metadata does not include the content of user prompts, uploaded images, or generated outputs where provider content logging is disabled or where the provider's applicable data-processing terms prohibit such content use. Where such metadata constitutes personal data, it is protected under applicable data processing agreements, confidentiality obligations, security measures, and transfer safeguards.

Data processors and third parties

We engage the following third-party service providers ("processors") who process personal data on our behalf under contractual obligations and appropriate data protection safeguards:

- **Supabase** — backend infrastructure including database, authentication, and storage of user-generated content.
- **Revenuecat** — subscription and in-app purchase management, including processing of purchase history, entitlement status, and subscription events.
- **OpenRouter** — routing and processing of user-provided text inputs,

AI-generated outputs, and uploaded images for AI-powered content generation, image/photo analysis, and flashcard generation. We configure OpenRouter requests to deny provider data collection and do not use free AI models or provider routes that may use user data for model training.

- **Vexo Analytics** — analytics and performance monitoring, including app usage events, device information, and interaction metrics to improve app features and user experience.
- **Sentry** — crash reporting and application stability monitoring, including collection of error logs, crash reports, device information, and diagnostic data necessary to detect, investigate, and fix application errors.
- **Expo (Expo Application Services and modules)** — application infrastructure services including push notification delivery, device information handling, background tasks, camera and media access, and diagnostic or telemetry services where applicable.
- **Google LLC / Apple Inc.** — authentication providers used for sign-in via OAuth, including processing of basic profile information such as name, email address, profile picture, and unique account identifiers.
- **OpenAI Ireland Ltd. / OpenAI OpCo, LLC (“OpenAI”)** — AI text-to-speech generation and other AI processing services where enabled. OpenAI processes submitted text and generated outputs on our behalf to provide the requested service. We do not enable optional OpenAI data-sharing, model-improvement, evaluation, fine-tuning, or inputs/outputs sharing settings for user data.

We **do not sell, rent, or trade** personal data to third parties for their marketing or commercial purposes.

Local device storage

The App may store limited information locally on your device. This may include authentication or session status, consent preferences, accepted versions of the Privacy Policy and Terms and Conditions, app settings, onboarding status,

language preferences, cached subscription or entitlement status, and learning-related app state needed for App functionality.

Local data is used to keep you signed in, remember your preferences, maintain App functionality, reduce loading times, and record consent choices. Some locally stored data may correspond to data also stored in our backend where required for account functionality, subscriptions, security, or compliance. Local data remains on your device until it is updated, cleared through App functionality where applicable, or removed when you uninstall the App.

Audit logs and data integrity

To ensure compliance, security, and the integrity of records:

- We keep **logs of changes** to key account data and actions (e.g., consent updates, account deletions or modifications, App activity changes).
- These logs **do not contain sensitive personal data** (e.g., emails, names, or profile pictures). They record **metadata only**, such as the non-personal fields which changed and timestamps.
- Logs may be updated if corrections are necessary; they are not immutable.
- The purpose of these logs is to:
 - Track system changes and support troubleshooting,
 - Demonstrate compliance with data protection obligations, and
 - Support auditing, accounting, or fraud-prevention activities where necessary.
- Logs are stored securely with appropriate technical and organizational measures to prevent unauthorized access or misuse.

Data security and access control

We apply appropriate technical and organisational measures to protect personal data, including but not limited to:

- **Encryption:** Sensitive data is encrypted at rest (including, where feasible, IBANs) and in transit using HTTPS/TLS.

- **Database security:** Row-level security (RLS) and strict database policies to prevent unauthorized READ/INSERT/UPDATE/DELETE operations.
- **Personnel access:** Access to personal data is restricted to authorized personnel only.

International transfers

Your personal data is primarily processed and stored within the EU. Some service providers (e.g., providers of push notification or infrastructure services) may be located or process data outside the EU. Where personal data is transferred outside the EU/EEA we use appropriate safeguards such as EU Standard Contractual Clauses (SCCs) or other legally recognized transfer mechanisms to ensure an adequate level of protection.

Your rights

Under GDPR you have the right to:

- Request access to your personal data.
- Request rectification of inaccurate data.
- Request erasure of your personal data, subject to legal exceptions (see Sections 8–9).
- Request restriction of processing.
- Object to processing based on legitimate interests (including profiling) — if you object we will cease processing unless we have overriding legitimate grounds.
- Request portability of data you have provided in a structured, commonly used, machine-readable format.
- Withdraw consent at any time where processing is based on consent (withdrawal does not affect processing that occurred before withdrawal).
- Lodge a complaint with a supervisory authority.

To exercise your rights, contact us at contact@linkoglot.eu. We will respond within the timeframes required by law (generally within one month).

Consent management and policy versioning

- We record the specific version of the Privacy Policy and Terms and Conditions you agreed to at the time of consent (version identifiers and timestamp).
- If the Privacy Policy or Terms and Conditions change materially, we will notify via a push notification, email, or an in-app announcement.
- We store consent evidence both locally (on the device as applicable) and persistently in our database so that consent history is demonstrable and auditable.

Opting out of optional data collection and sharing

Marketing messages, promotional messages, engagement notifications, and optional product updates are sent only where you have given the required **marketing consent**. Where permitted by law and subject to your consent and communication preferences, we may send these communications by email, push notification, in-app message, or other available communication channels.

Withdrawing consent for marketing, engagement notifications, or optional communications does not prevent us from sending you important service-related communications where they are necessary for the operation, security, legal compliance, or administration of the App. These may include communications about your account, purchases, subscriptions, renewals, failed payments, refunds, AI Credits, changes to our Terms and Conditions or Privacy Policy, security notices, account deletion, service availability, abuse prevention, and other important non-marketing matters. Withdrawal of consent does not affect the lawfulness of processing based on consent before it was withdrawn.

Service-related communications are not marketing communications. We process and send them where necessary for the performance of our contract with you, compliance with legal obligations, or our legitimate interests in operating, securing, and administering the App.

Some communication channels may not be available. We can only send communications through channels that are available to us and enabled by you or your device, platform, or service provider. If a communication channel is unavailable, disabled, blocked, incorrect, or not provided, we may be unable to send communications through that channel and may use another available method where permitted.

We do not use personal data for third-party advertising or sell, rent, or trade personal data to third parties for their marketing purposes.

Data breach notification

In the event of a personal data breach that is likely to result in a risk to the rights and freedoms of individuals, we will notify the competent supervisory authority, Urząd Ochrony Danych Osobowych (UODO), and affected users where required by applicable law, without undue delay and within statutory time limits (including the 72-hour period where applicable under GDPR).

We take reasonable technical and organisational measures to prevent, detect and mitigate security incidents and will respond appropriately if a breach occurs.

Changes to this Privacy Policy

We may update this Policy to reflect changes in our practices, legal requirements, or features of the App. Material changes will be communicated to users, and where required by law, renewed consent will be obtained prior to continued use. We will notify users of material changes to this Policy, and continued use of the App after an updated version is published constitutes acceptance where permitted by law.

Contact information and complaints

If you have questions, wish to exercise your rights, or want to submit a complaint:

Data Controller: Mateusz Jakub Muszarski

Address: Osiedle Konstytucji 3 Maja 21/4, Starogard Gdański 83-200, Pomorskie, Poland

Linkoglot contact email: contact@linkoglot.eu

Controller administrative email: mat.muszarski@gmail.com

You also have the right to lodge a complaint with the supervisory authority: **Urząd Ochrony Danych Osobowych**.