

Privacy Policy – Mythic Cards

Version: privacy_v2026_09_launch_candidate_1
Artifact: la1_6582693587cdeb9b8b13a7a6edf96f766dba0e3a70c99cf9c0c6c9ccb5e3288e
Body SHA-256: 6bfca0f90141eea7c8a28773d9f0f95069599dfcc0a21107cc707a25acb2a7e7

Privacy Policy – Mythic Cards

Last updated: 26 September 2026

1. Controller

The controller within the meaning of the EU General Data Protection Regulation (GDPR) is:

Pacoma Creative Labs – Owner: Christian Renschler

c/o Impressumservice Dein-Impressum

Stettiner Str. 41

35410 Hungen

Germany

Phone: 01579-2341658

Email: info@mythiccards.ai

Website: <https://mythiccards.ai>

2. Scope

This Privacy Policy applies to the website and platform “Mythic Cards” (mythiccards.ai) and all related processing of personal data. Our service is offered worldwide. For users in the EU/EEA, the requirements of the GDPR apply in particular.

3. Overview: what data we process and why

We process personal data in order to provide the platform (account, generation, storage/sharing, waitlist/capacity handling, public features, reports/moderation), process payments, ensure security, keep legally required records, handle support and cancellation requests, and—only with your consent—to analyse the usage of our website/platform via Firebase Analytics.

4. Hosting, website delivery and server log files (Vercel)

Our website is provided via Vercel. When you access the site, technically necessary data may be processed (e.g., IP address, date/time, requested content, referrer, browser/device information). Purposes: delivery of content, stability, IT security, error analysis and abuse prevention.

Legal basis: Art. 6(1)(f) GDPR (legitimate interest in operating a secure and reliable service).

Retention: server log data is retained only as long as necessary for security, stability, abuse prevention and incident investigation, unless longer retention is legally required.

5. Account, registration and login (Firebase Auth / Google Login)

To use core features, a user account is required. We process in particular: email address, user ID, login timestamps, and—if you use Google Login—display name/profile picture, as well as security/authentication data.

Purposes: account administration, authentication, abuse prevention and operation of the platform.

Legal basis: Art. 6(1)(b) GDPR (contract/account) and Art. 6(1)(f) GDPR (security).

6. Platform data (Library, Discovery Board, Public Profile, Showcase, likes, Copy feature, Race editor, waitlist, public interactions)

We process content and metadata created through your use of the platform, e.g., card title,

description/prompts, rarity, frame, timestamps, creator name, Showcase selection, likes, visibility status (private/unlisted/public), copy actions, Copied Card metadata, race definitions (name, attributes), public profile information, Discovery and ranking signals, like counts, copy counts, Creator Credit allocation data, and waitlist entries. Public content can generate public or internal interaction data such as likes, reports, copy interactions, Creator Credits, Discovery signals, Top Cards/ranking signals, and moderation signals. Copied Cards are private copies intended for the copying User's Library and are not intended for public platform surfaces.

For logged-in Users, a waitlist entry may include the User ID, account email address, selected plan, source, invite status and email sending metadata. For email-only waitlist entries without notification consent, we store only a hashed version of the normalized email address and the selected plan/source so that demand can be measured without storing the raw email address. If you explicitly choose to be notified by email when beta spots become available, we may store the raw email address you entered, the consent status/version/time, selected plan/source, invite status and email sending metadata for that waitlist notification purpose.

If you publish content on the Discovery Board or make cards visible through your Showcase/Public Profile, it is visible to other users. Please do not publish personal data of third parties.

A Card produced by paid Reference Edit starts private. If eligible, you may later choose to publish it through the platform's public presentation features. This makes the output's public presentation available; it does not automatically publish the source reference files or their private provenance and integrity records. The output itself may visibly reflect material from the references.

Purposes: providing platform features, moderation/abuse prevention, accounting and allocation of Credits and Race Tokens.

Legal basis: Art. 6(1)(b) GDPR (contract) and Art. 6(1)(f) GDPR (security, abuse prevention).

6.1. User reports, moderation and takedown data

If Users report public or otherwise publicly accessible cards, or if content is reviewed for moderation, rights protection, safety, or abuse prevention, we may process report and moderation data. This can include reporter ID, card ID/image ID, owner ID, report reason, optional report details, source/context of the report, timestamps, report status, minimal card snapshots/card metadata, reviewedAt, reviewedBy, actionTaken, adminNote, moderationStatus, publicBlocked, publicBlockedReason, publicBlockedNote, publicBlockedBy, publicBlockedAt, reportCount, lastReportedAt, restoredAt, restoredBy, and restoreReason.

Admins, moderators, support staff, or other authorized operators may review reports and related card metadata to enforce the Content Policy, protect rights, keep public areas safe, prevent abuse, document moderation decisions, and comply with legal obligations. Report and moderation records may be retained for documentation, security, rights-protection, legal defence, and abuse-prevention purposes for as long as permitted or required by law.

7. AI generation and Reference Edit (OpenAI API): prompts, reference images, outputs

We use the OpenAI API to generate digital cards. Ordinary Generate sends your prompts/descriptions and selected generation settings without selected image references. Where available, Card and Freestyle Reference Edit uses one to four verified image references. These may be eligible existing Mythic Cards that you own in the platform, private uploaded images, or a combination of both.

For Reference Edit, actual verified reference image data may be transmitted to OpenAI together with your prompts, generation instructions and technical metadata for image-guided generation or editing. This is not limited to style analysis. When you select an existing Card, we check access and eligibility and resolve the stored original for processing. Its use as a reference does not turn it into a temporary upload. Generated results are provided to your account; publishing an eligible output does not automatically publish its source references or private processing records.

We may store private reference identities, source relationships, order and roles, and integrity information needed to identify and verify the inputs to an accepted request. This may include file

locations, file versions and checksums. These records are distinct from the image files themselves and may remain after temporary image bytes are removed. We also process generation metadata such as the selected model and quality, processing status, final Credit price and its components, wallet and Monthly Generation Allowance charges, and any failure settlement.

Necessary operational records may include request identifiers, timestamps, error and retry information, provider usage and cost information. They support execution, accounting, refunds, security, abuse prevention, error analysis and support. These operational records are separate from optional website analytics described in Section 10 and are not published with the output.

Legal basis: Art. 6(1)(b) GDPR (performance of contract) and Art. 6(1)(f) GDPR (security, abuse prevention and technical stability); applicable accounting and legal record-keeping is described in Sections 8 and 9.

Prompts, jobs, outputs, temporary uploads and private provenance records have different retention lifecycles, as described in Section 13. Cleanup of temporary uploads is asynchronous and may wait for active requests, retries or a safety period. We do not promise immediate deletion after generation.

OpenAI's processing and retention are subject to the applicable API terms, policies, service and data controls. Provider-side records may be retained for operating and securing the service or meeting legal obligations. We do not promise Zero Data Retention, EU-only processing, no provider retention or an unconditional exclusion of training use. Any applicable restrictions depend on the provider's terms and the data controls in effect for the service. OpenAI's API data-control information is available at:

<https://developers.openai.com/api/docs/guides/your-data>

7.1. AI Enhanced Print-Ready Upscale (Replicate / Topaz)

If you use AI Enhanced Upscale for Print-Ready exports, image files, temporary image URLs and technical metadata may be transmitted to an external upscaling or image enhancement provider. The current provider is Replicate / Topaz. The processing is carried out for the purpose of creating the requested AI-enhanced Print-Ready export, technical processing, error analysis, abuse prevention and cost/Credit attribution. The legal basis is Art. 6(1)(b) GDPR (contract performance) and, where required, Art. 6(1)(f) GDPR (security, abuse prevention and technical stability). Temporary input and output artifacts are retained only for as long as needed for export creation, technical safety, support or legal obligations.

8. Payments and subscriptions (Stripe)

For subscriptions and one-time purchases (Credit Packs) we use Stripe as a payment service provider. Stripe processes payment data (e.g., card data) under its own responsibility; we typically receive transaction and status information (e.g., payment status, subscription status, invoice/receipt data) and store necessary mapping data (e.g., Stripe customer/subscription IDs) in our database.

Purposes: payment processing, fraud prevention, accounting and record-keeping.

Legal basis: Art. 6(1)(b) GDPR (contract) and Art. 6(1)(c) GDPR (legal obligations, e.g., commercial and tax retention).

Retention: invoice/accounting data typically up to 10 years (statutory retention); other payment/subscription mapping data is retained for as long as needed for the customer relationship, fraud prevention, dispute handling and legal defence.

9. Storage in Firebase (Firestore, Storage) and technical processes (Cloud Functions)

We use Firebase (Google) for authentication, database (Firestore), file storage (Storage) and Cloud Functions. Depending on usage, this may include account/profile information, platform content (e.g., cards, races, decks), and technical data (e.g., job status, processing data).

We also maintain internal records and processes, e.g.: "checkoutConsents" (e.g., purchase/withdrawal/consent records), "legalAcceptances" (acceptance of Terms/Privacy), "contentReports" and moderation records, subscription cancellation/support request records, "emailOutbox" (internal sending/notification queue), and legal notification or legal update records where such notifications are prepared or sent.

Private processing records may also link an accepted generation request to its verified references, source integrity information and output. Financial records may document the final Credit price and its components, wallet debits, allowance grants and billing periods, allowance usage, and whether wallet Credits or allowance were restored after a failure. Wallet restoration and allowance restoration are recorded separately; an allowance adjustment may be zero when its charged period is no longer applicable. Legal records may document the exact document versions and text or PDF integrity information presented, their applicable requirements, and when and by whom acceptance was given. We use these limited records for execution, accounting, refunds, security, support, legal defence and compliance. They are private evidence, not additional public Card information. Retaining them does not keep deleted temporary image files available or recreate a deleted account.

Legal basis: Art. 6(1)(b) GDPR (contract), Art. 6(1)(c) GDPR (record-keeping obligations) and Art. 6(1)(f) GDPR (operation/security).

10. Cookies, consent, Consent Mode foundation and Firebase Analytics (consent)

We use cookies and similar technologies. Some are technically necessary (e.g., for login, security, consent storage, payment flows or platform operation). Others are used only with your consent.

Consent management: We use a consent banner and Cookie Settings. Your current choice is stored via the cookie "mythic-cards-consent-v2". Older choices may also be read from the legacy cookie "mythic-cards-consent" so that previous analytics choices are not lost abruptly. The current consent categories are:

- necessary: required for website/platform operation and always active.
- analytics: optional; controls Firebase Analytics and analytics events.
- marketing: optional; prepared for future advertising or conversion tags, but no real Meta, TikTok or Google Ads pixel scripts are active unless separately configured and enabled after the required legal and consent setup.

You can change or withdraw optional analytics or marketing consent at any time with effect for the future via Cookie Settings.

Firebase Analytics: Firebase Analytics is technically integrated but is only initialised after analytics consent (consent-gated). In this context, online identifiers (e.g., cookie IDs), device/browser information and usage events may be processed to understand usage and improve the platform.

Google Consent Mode foundation: the platform may maintain a local consent-state foundation for Google Consent Mode v2. This sets default states such as `ad_storage`, `analytics_storage`, `ad_user_data` and `ad_personalization` to denied and updates the local consent state according to your analytics and marketing choices. This foundation alone does not mean that Google Ads, Google Tag Manager, Meta Pixel or TikTok Pixel scripts are active.

Tracking and event data minimisation: where analytics or future marketing events are used, we intend to send only non-sensitive product and funnel metadata such as page views, plan views, checkout starts, purchase/subscription status, generation start/completion status, amount, currency, plan type or similar technical event information. We do not intend to send prompts, card names, image URLs, uploaded images, free-text report details, user emails or sensitive user-generated content in marketing events.

Legal bases: Technically necessary cookies: Art. 6(1)(f) GDPR (operation/security). Analytics and optional marketing technologies: Art. 6(1)(a) GDPR (consent) in conjunction with § 25(1) TDDDG, insofar as information is stored on or accessed from your end device.

Examples of (possible) cookies: consent: mythic-cards-consent-v2 and legacy mythic-cards-consent; analytics: `_ga`, `_ga_*`, `_gid` or Firebase/Google Analytics-related identifiers (depending on setup and only after consent); Stripe: `__stripe_mid`, `__stripe_sid` (depending on the payment flow). Note: the cookies

actually set may vary depending on device/browser/integration.

We do not currently use Google Tag Manager, Meta/Facebook Pixel, TikTok Pixel, Sentry, PostHog, Mixpanel, Plausible, Umami, Hotjar, Clarity, Vercel Analytics/Speed Insights, Firebase Messaging, Firebase Performance Monitoring, Crashlytics, Remote Config or In-App Messaging.

11. Recipients and processors

We use service providers (processors) who process data on our behalf, in particular for hosting, Firebase/Google, Stripe, OpenAI and, where AI Enhanced Print-Ready Upscale is used, Replicate/Topaz. We have the required data protection agreements in place (in particular processing under Art. 28 GDPR) or comparable contractual frameworks.

Key service providers: Vercel (hosting), Google Firebase (Auth/Firestore/Storage/Functions/Analytics), Stripe (payments), OpenAI (AI generation and Reference Edit), Replicate/Topaz (AI Enhanced Print-Ready upscaling, where used).

12. International data transfers (e.g., USA)

Depending on the service provider, processing may take place in countries outside the EU/EEA (in particular the USA). In such cases we use appropriate safeguards (e.g., Standard Contractual Clauses (SCCs) or—where applicable—adequacy decisions). Further information can be found in the privacy notices/DPA of the

respective providers.

13. Retention / deletion

We store personal data only for as long as necessary for the respective purposes. Specific retention periods are defined—depending on the data category—as follows:

- Account data: until account deletion; thereafter only as long as needed for technical processing, backups, security, or legal obligations, unless statutory retention obligations apply.
- Generated content/cards and existing Card originals: retained to provide the Library and related features until deletion is requested or the account is deleted, subject to necessary deletion processing and the retention grounds below. Selecting an existing Card as a reference does not cause its original to be deleted when that generation ends. Public presentation files are handled separately when public visibility is removed; previously obtained copies or links may require separate handling.
- Temporary uploaded reference images: staged privately for verification and generation. Their lifetime depends on expiry, use in accepted or active requests, retries and cleanup safety periods. Cleanup runs asynchronously when the files are no longer required. It is not immediate deletion on completion; limited retention may also be needed for support, security, abuse prevention or legal obligations.
- Private reference-provenance and integrity records: retained separately from temporary image bytes where needed to identify inputs to an accepted request, verify execution, handle failure settlement, provide support, investigate abuse or meet legal obligations. Removing an upload does not necessarily remove these records at the same time.
- Print-Ready exports: temporary export artifacts are retained only as long as needed for delivery, repeat download, support, security, or legal obligations; currently the newest 10 Print-Ready exports per user are kept and older artifacts may be deleted automatically.
- Logs/security data: retained only as long as needed for security, incident investigation, or abuse prevention.
- Billing/accounting data: typically up to 10 years. Relevant records may include Credit charges, allowance grants, charged allowance periods and failure settlements. They may remain after deletion of the related image, job or account where needed for accounting, refunds, disputes or legal obligations.
- Consent/record data (e.g., legalAcceptances/checkoutConsents): retained as long as needed to document consents, the exact legal versions accepted, contract performance, legal defence, or statutory obligations.

- Report/moderation/takedown records: retained as long as needed to review and document reports, moderation actions, rights-protection decisions, abuse prevention, security, legal defence, or legal obligations.
- Support, contact and cancellation request records: retained as long as needed to process the request, document the result, comply with legal obligations, resolve disputes, or defend legal claims.
- Cookie/consent choices: retained as long as needed to remember and document your current consent choice and to operate Cookie Settings, unless you reset cookies or change your choice earlier.

Account deletion starts the relevant deletion processes; it does not guarantee immediate erasure of every copy, backup or financial, legal, technical or security record. Access and retention are limited to the remaining necessary purposes and applicable legal requirements. Retained evidence does not restore a deleted account or grant new Credits or allowance. Service providers apply their own applicable processing and retention terms. Other Users' existing private Copies and data already obtained outside the platform are not automatically erased by deletion of the original account.

14. Your rights

Subject to the statutory requirements, you have the following rights: access (Art. 15 GDPR), rectification (Art. 16 GDPR), erasure (Art. 17 GDPR), restriction of processing (Art. 18 GDPR), data portability (Art. 20 GDPR), objection (Art. 21 GDPR), and withdrawal of consents (Art. 7(3) GDPR). To exercise your rights, please contact us using the details above.

15. Right to lodge a complaint with a supervisory authority

You have the right to lodge a complaint with a data protection supervisory authority. For Baden-Wuerttemberg (Germany), the competent authority is: The State Commissioner for Data Protection and Freedom of Information Baden-Wuerttemberg (LfDI BW), Heilbronner Strasse 35, 70191 Stuttgart, Germany, email: poststelle@lfdi.bwl.de.

16. Data security

We implement technical and organisational measures to protect your data from loss, misuse and unauthorised access (e.g., encryption, access controls, logging, role/permission concepts).

17. Changes

We may update this Privacy Policy if our processing activities, legal requirements or service providers change. The current version is available on our website.