DashaMap Privacy Policy

Full English Controlling Version

Version: 1.4

Last Updated: October 26, 2026

Effective Date: upon coordinated publication with the corresponding service configuration

Table of Contents

1. Data Controller and Contact Details

2. Scope of Application

3. Key Definitions

4. Categories of Personal Data Processed

5. Sources of Data

6. Purposes of Processing

7. Legal Bases for Processing

8. AI/LLM: Use of AI, Data Sent, and Limitations

9. Cookies and Similar Technologies

10. Data Recipients and Roles

11. International / Extra-EEA Transfers

12. Retention Periods and Retention Criteria

13. Security Measures

14. Data Subject Rights

15. Deletion Requests and Practical Effects

16. Minors and Child Data

17. Communications

18. Automated Anti-Abuse, Fraud Prevention, and Security Signals

19. Processing on Behalf of Business / White-Label Customers

20. Certified Astrologers, Partner/Dealer, Referral, Coupon, and Application Flows

21. Alignment with ToS, AUP, Cookie Policy, DPA, AI Notice, and Disclaimer

22. Changes to this Privacy Policy

23. Language and Controlling Version

24. Contact Details

Annex A. Sub-Processor List

Annex B. Data Retention Schedule, Deletion, and Backups

Annex C. Extra-EEA Transfers, Safeguards, and Transparency

Annex D. Summary of Technical and Organisational Security Measures

Annex E. DSAR Procedure and Identity Verification

DashaMap Privacy Policy

This Privacy Policy describes how GLOBAL MOUNTAIN GROUP LLC processes personal data in connection with DashaMap, including account data, birth data, profiles, usage data, generated outputs, payment and billing information, technical logs, support communications, AI-assisted features, gifts, one-shot reports, referral/coupon tools, Certified Astrologers flows, Partner/Dealer flows, and business/white-label features where available.

This Policy is drafted for operational transparency and is intended to be read together with the Terms of Service, Astrological Disclaimer, AI Transparency & Compliance Notice, Cookie Policy, Acceptable Use Policy, Refund / Billing / Subscription / Credits Policy, and, where applicable, any Data Processing Addendum or written business agreement. This Policy is an information notice, not a request for blanket consent. Reading it or using the Service does not constitute consent to optional analytics, promotional communications or other processing requiring a separate choice.

References to GDPR articles are included for transparency and do not limit any additional obligations or rights under applicable law. Mandatory, non-waivable data-protection and consumer rights remain unaffected.

1. Data Controller and Contact Details

The Data Controller is GLOBAL MOUNTAIN GROUP LLC.

Registered office: 30 N Gould St #39973, Sheridan, WY 82801, United States.

Company ID: 2023-001208525 General email / Privacy contact: info@globalmountain.group Website: www.globalmountain.group Recommended email subject for privacy requests: "Privacy - DashaMap" or "GDPR Request - DashaMap".

DPO (Data Protection Officer): as of the update date of this Policy, no DPO has been appointed. If an appointment becomes mandatory or is made for organizational reasons, the relevant contact details will be published in this section or in the Legal Center.

Representative

We value your privacy and your rights as a data subject and have therefore appointed Prighter Group with its local partners as our privacy representative and your point of contact for the following regions:

European Union (EU)

Prighter gives you an easy way to exercise your privacy-related rights (e.g. requests to access or erase personal data). If you want to contact us via our representative, Prighter or make use of your data subject rights, please visit the following website:

https://app.prighter.com/portal/15940114520

UK representative: no appointed UK representative is identified in this version. The Controller's direct privacy contact remains info@globalmountain.group. That contact does not substitute for a UK representative where appointment is required. A separate UK assessment applies; this notice does not claim that an exemption has been established.

2. Scope of Application

This Policy applies to personal data processed through the DashaMap website, application, account areas, workspace, dashboard, My Path, Sinfonia, Oracle, PDF exports, Sacred Seal or similar exports, Magic Links, shareable links, gift flows, one-shot digital report flows, referral/coupon tools, Certified Astrologers application or activation flows, Partner/Dealer flows, support, email communications, and any business/white-label/client portal functions where available.

Business, white-label, enterprise, Partner/Dealer, and Certified Astrologers features may be available only in certain regions, plans, phases, or after approval. References to such features do not guarantee availability to every user.

Where data is entered about another person, the user or business customer that enters the data remains responsible for having a valid legal basis, notice, authorization, consent, or other lawful ground as required by applicable law.

3. Key Definitions

• Service: the DashaMap platform and related functionalities, including website/app, accounts, workspace, generations, exports, reports, shareable links, plans, add-ons, gifts, one-shot reports, and support.

- User: any natural person who accesses or uses the Service, including visitors, registered users, subscribers, gift recipients, invited users, authorized users under a business account, and applicants to relevant programs.
- Business / white-label customer: a professional entity using DashaMap for its own team or toward clients/end customers, where such features are available and contractually enabled.
- Souls / Profiles: profiles created in the Service, including profiles relating to the user, pets, children, family members, clients, or other third parties, where permitted by the Service and applicable law.
- Birth data: date of birth, time of birth, place of birth, and derived coordinates, time zones, or deterministic calculation results needed for the requested features.
- Output: content generated, calculated, compiled, or reformulated by the Service, including texts, timelines, symbolic interpretations, reports, PDFs, notifications, summaries, or AI-assisted content.
- Credits / Sparks / quotas: contractual usage entitlements, counters, allowances, or consumption units used to access certain features, generate outputs, or export PDFs, as described in the billing policies and product UI.
- Gift recipient: a person who receives or claims access to a gift product, gift link, or gift entitlement purchased by another person, where such feature is available.
- One-shot report: a one-time digital report or paid digital product that does not automatically create a recurring subscription unless clearly stated at checkout.
- Certified Astrologer / Partner / Dealer: a professional, applicant, referral participant, or business collaborator using dedicated flows, if and when approved or enabled.
- Magic Link / shareable link: a URL generated by the Service for access to or sharing of content, with possible expiration, revocation, watermarking, or access controls.
- Third-party providers: technical or commercial providers that may process data as processors, sub-processors, or independent controllers, depending on the function.

4. Categories of Personal Data Processed

4.1 Account and Identification Data

- Email address.
- First name, last name, nickname, display name, or pseudonym, if entered.
- Language, locale, preferences, settings, and notification choices.
- User ID, account ID, profile ID, tenant ID, or other technical identifiers.
- Authentication data managed through authentication providers; the Controller should not see passwords in plain text.
- Billing identity and compliance information where required for payments, receipts, fraud prevention, disputes, tax/accounting, or legal obligations.

For ordinary use, the visible profile name does not always need to be a legal name. Users may use a nickname or pseudonym, provided it is not deceptive, unlawful, infringing, impersonating, or contrary to the ToS/AUP.

Billing and payment data must be accurate where required.

4.2 Birth Data and Profiles ("Souls")

- Date of birth.
- Time of birth, if provided or required by the feature.
- Place of birth, city/country, and derived coordinates or time-zone information where necessary.
- Profile elements linked to calculation or personalization, such as goals, tags, preferences, notes, diary entries, or context entered by the user.
- Derived deterministic results, timelines, cycles, windows, or calculation outputs used by the Service.
- Pet profile data for Companion Soul features, where available.
- Child or family profile data for Child Evolution Atlas or family features, where entered by an adult with lawful authority.

Birth data is normally not a special category under Article 9 GDPR by itself, but it can be highly identifying and operationally sensitive. DashaMap treats it with enhanced care through minimization, access controls, and security measures proportionate to the Service.

4.3 Usage Data and Generated Content

- Actions and requests performed in the Service, including activations, generations, report creation, PDF export, gift claim, one-shot report creation, and use of shared links.
- User-entered content, prompts, questions, notes, diary entries, completed fields, and support attachments voluntarily sent.
- Outputs generated by the Service, including timelines, interpretations, summaries, reports, notifications, PDFs, and AI-assisted text.
- Plan status, quota status, Credits/Sparks usage, add-on balances, refund/restore events, and feature eligibility.

Outputs linked to an account or identifiable profile are treated as personal data to the extent required by applicable law.

4.4 Payment and Billing Data

- Subscription status, renewals, cancellations, upgrades, downgrades, add-ons, one-shot purchases, gift purchases, gift claims, refunds, coupons, referral benefits, and taxes where applicable.
- Transaction history, transaction identifiers, customer ID, subscription ID, invoice or receipt identifiers, and payment status.
- Administrative, fiscal, billing, and dispute-related information required for accounting, compliance, chargeback handling, and fraud prevention.
- Payment outcome and anti-fraud/compliance signals from payment providers such as Stripe or equivalents.

Complete payment card data are normally handled by the payment provider and are not fully stored by the Controller.

4.5 Technical, Security, and Log Data

- IP address, user agent, device/browser type, HTTP request data, session and account events.
- Access logs, usage logs, error logs, stack traces where applicable, and performance telemetry.
- Security events, anti-fraud signals, anti-abuse signals, rate patterns, anti-bot indicators, and suspicious activity indicators.
- Cookie and similar technology identifiers as described in the Cookie Policy.

4.5.1 Optional Analytics and Consent Controls

DashaMap first-party analytics can record permitted page paths, event names and timestamps, language, country information, referring host, campaign parameters, referral codes and pseudonymous visitor/session identifiers. Integrated events can concern registration, free tests, checkout, gifts, one-shot purchases, payment outcomes and delivery. Depending on the flow, an event may be associated with an authenticated user ID or transaction/resource ID. These detailed records are not represented as anonymous.

The analytics event pipeline restricts fields such as names, email addresses, birth data, questions, prompts and generated answers. It does not store raw IP addresses as analytics fields; infrastructure providers can still receive network information when processing requests. Security hashes and infrastructure logs are separate from optional analytics.

The browser stores the current cookie choice and its timestamp. Server controls store a session consent-expiry deadline and revoked visitor identifiers with revocation timestamps. A necessary pending-withdrawal marker can remain in browser storage until server confirmation. These records enforce preferences; they are not a complete historical register of every banner version and consent choice.

4.6 Communications, Whispers, and Notifications

- Communication and notification preferences.

- Data necessary to send operational emails, receipts, security alerts, service notifications, Whispers, gift emails, one-shot delivery emails, application notifications, or partner/referral communications.
- Delivery/failure logs for deliverability, support, fraud prevention, and security.

4.7 Support, Assistance, Applications, and Program Data

- Support requests, troubleshooting history, screenshots, attachments, and related correspondence.
- Certified Astrologers application or activation data, where a user applies to be listed, verified, activated, approved, refused, suspended, renewed, or otherwise managed.
- Partner/Dealer application, approval, referral, commission, payout, anti-fraud, compliance, and internal note data, where such program is available.
- Public directory or public profile information only where the user/applicant submits it for publication or where publication is part of the approved feature terms.

Partners, Dealers, and Certified Astrologers must not include unnecessary personal data, client birth data, emails, phone numbers, sensitive data, or private client content in internal notes or communications unless expressly required and lawful.

4.7.1 Contact Form Delivery

The contact form sends the entered name, email address and message through Resend to support@dashamap.com. The sender's supplied email address is used as the Reply-To address so support can respond. Email content is processed by the delivery service and support mailbox.

The application's delivery-control tables store a request identifier, keyed hashes, delivery status and technical timestamps/counters. Those tables do not store the message, email address or raw IP address. Hashes support duplicate prevention and rate limits. This restriction does not mean that message content is absent from the email service or mailbox; those copies have separate purposes and retention requirements.

4.8 Data We Ask You NOT to Provide

Unless expressly requested by a structured field and legally necessary, do not enter unnecessary sensitive or high-risk data in free-text fields, prompts, notes, support tickets, or partner/internal notes. Examples include health details, psychological diagnoses, medical records, document numbers, credentials, OTP codes, seed phrases, full payment card data, banking secrets, criminal data, political opinions, religious beliefs, sexual orientation, trade secrets, or confidential third-party data.

If an AI output or user-created workflow suggests entering excessive or unnecessary data, official platform fields, this Privacy Policy, the ToS, the AUP, and the DPA where applicable always prevail. Lack of a technical block does not mean that entering such data is necessary, authorized, or lawful.

5. Sources of Data

- Directly from the user during registration, profile completion, prompts, notes, report requests, checkout, support, application, referral, or partner flows.
- From use of the Service, including logs, events, feature use, credits/quota use, shared links, gift claim activity, and preferences.
- From payment providers for transaction status, identifiers, invoice/receipt data, subscription status, chargebacks, disputes, and anti-fraud signals.
- From technical providers such as hosting, authentication, monitoring, email delivery, security, and AI/LLM providers.
- From other users or business customers who enter third-party data into profiles or client flows. In that case, the person or entity entering the data remains responsible for the lawful basis and notice obligations unless otherwise agreed in writing.

6. Purposes of Processing

6.1 Provision of the Service and Core Features

- Create and manage accounts, sessions, preferences, and profiles/Souls.
- Calculate timelines, cycles, windows, memories, deterministic results, and related structures.
- Provide My Path, Sinfonia, Oracle, Companion Soul, Child Evolution Atlas, reports, exports, PDFs, Magic Links, shareable links, and related features where available.
- Generate, compile, store, display, deliver, or regenerate outputs requested by the user.
- Personalize language, locale, and settings.

6.2 Subscriptions, Billing, Credits/Sparks, Gifts, and One-Shot Products

- Activate plans, renewals, cancellations, upgrades, downgrades, add-ons, purchased Credits/Sparks, and included quotas.
- Process one-shot digital reports and gift products, including purchase, delivery, claim, activation, expiration, support, and fraud prevention where applicable.
- Measure consumption of Credits/Sparks, quotas, PDFs, reports, and feature eligibility.
- Handle billing, receipts, taxes, accounting, refunds, failed generations, non-delivery events, disputes, and chargebacks.
- Restore or refund Credits/Sparks where the applicable policy and product logic require it because a paid task failed and was not delivered.

6.3 Security, Abuse Prevention, and Platform Integrity

- Protect accounts, profiles, outputs, PDFs, shared links, magic links, payments, gifts, and partner/referral flows.
- Prevent fraud, account takeover, scraping, abuse, unauthorized automation, bypass of paywalls/credits, duplicate-click errors, and misuse of technical systems.
- Apply technical safeguards such as rate limits, anti-bot measures, verification challenges, throttling, temporary restrictions, IP/device/network signals, and anomaly detection when necessary for security and service integrity.
- Investigate incidents, abuse, security issues, suspicious activity, or violations of the ToS/AUP.

Security and anti-abuse controls are intended to protect the Service, users, and technical supply chain. They do not by themselves create artificial daily consumption caps on purchased entitlements; any feature limits or consumption rules are governed by the product UI, plan terms, ToS, and Refund / Billing / Subscription / Credits Policy.

6.4 Support and Assistance

- Respond to tickets, privacy requests, security reports, billing inquiries, gift/one-shot delivery issues, and application/partner requests.
- Troubleshoot errors, access issues, failed generations, failed PDF deliveries, and account recovery.
- Send operational communications about account, payment, maintenance, security, delivery, application, or policy matters.

6.5 Product Improvement, Analytics, and Reliability

Optional first-party measurement and Vercel Web Analytics, where enabled, require a valid affirmative analytics choice. Missing, refused, invalid or expired choices do not authorise optional browser collection. Necessary error handling and security processing are assessed separately and must not be used to bypass that choice.

First-party analytics support understanding visits, product use and permitted conversion paths. Detailed data are subject to the 12-calendar-month rule in Section 12 and Annex B. Restricted monthly totals support longer-term comparisons. Aggregation and rounding reduce detail but are not, by themselves, proof of irreversible anonymisation.

Vercel Web Analytics is a separate service; the first-party deletion job does not delete Vercel reports. Its visitor-identifier lifetime must not be confused with retention of provider-held statistical reports.

6.6 Legal Compliance and Defense

- Comply with fiscal, accounting, administrative, privacy, consumer, cybersecurity, sanctions, and other legal obligations.
- Respond to valid authority requests or legal process.
- Defend the Controller, users, and third parties in complaints, disputes, chargebacks, litigation, fraud cases, and abuse investigations.
- Maintain records necessary for auditability, security, dispute handling, and enforcement of legal documents.

7. Legal Bases for Processing

Where GDPR applies, processing may rely on one or more of the following legal bases, depending on the specific purpose.

7.1 Performance of a Contract or Pre-Contractual Measures - Art. 6(1)(b) GDPR

- Account creation and management.
- Provision of requested features, calculations, reports, outputs, PDFs, gifts, one-shot products, shared links, workspace, and support connected to the Service.
- Management of subscriptions, billing, Credits/Sparks, quotas, add-ons, refunds, cancellations, and feature eligibility.
- Essential operational communications for security, service delivery, maintenance, payment, and account management.

7.2 Legal Obligation - Art. 6(1)(c) GDPR

- Fiscal, accounting, administrative, consumer, and regulatory obligations.
- Responses to valid orders or lawful requests from authorities.
- Mandatory retention required by applicable law.

7.3 Legitimate Interests - Art. 6(1)(f) GDPR

- Security, fraud prevention, anti-abuse, anti-scraping, infrastructure protection, and technological supply-chain protection.
- Error monitoring, service resilience, operational continuity, uptime, and hardening.
- Protection of intellectual property, contractual rights, evidence, and defense in court.
- Necessary technical analyses for performance and reliability, subject to minimization, a documented legitimate-interest assessment and applicable device-access rules. This ground does not replace the analytics-consent requirement described in Sections 6.5 and 9.

7.4 Consent - Art. 6(1)(a) GDPR

- Non-necessary cookies and similar technologies, where required.
- Marketing or promotional communications, where required.
- Optional features or disclosures for which applicable law requires consent.

Consent may be withdrawn at any time without affecting the lawfulness of earlier processing. Continued storage after withdrawal requires its own lawful justification. Where consent was the only basis and no other lawful ground applies, the personal data must be erased without undue delay; the routine retention deadline is not permission to wait.

7.5 Special Categories and Criminal-Offence Data

DashaMap does not request unnecessary health, religious, political, sexual-orientation or other special-category data for ordinary use. Processing within Article 9 GDPR requires an applicable Article 9 condition as well as an Article 6 basis. Criminal-conviction and offence data are governed separately by Article 10 GDPR. Entering data in a free-text field does not create a lawful basis or transfer the Controller's obligations to the user. Birth data can be highly identifying even where it is not special-category data by itself. Users should avoid unnecessary sensitive information; any such data received must be assessed and handled under the applicable requirements.

8. AI/LLM: Use of AI, Data Sent, and Limitations

8.1 What AI Does in DashaMap

DashaMap may use AI/LLM systems to generate, summarize, reformulate, explain, or structure interpretive and narrative text. AI may assist features such as Oracle, interpretive explanations, report texts, summaries, Whispers, gift recipient experience, one-shot reports, and support/editorial text.

Deterministic calculations, where present, are conceptually separate from AI. The engine calculates; AI may narrate or explain. AI must not be treated as a source of factual certainty, professional advice, medical/veterinary/psychological diagnosis, legal advice, financial advice, or a decision engine.

8.2 What Data May Be Included in Prompts

- Relevant portions of birth data or derived deterministic results, when necessary for the requested feature.
- User questions, notes, prompts, language, locale, style settings, and selected profile context.
- Report structure, template instructions, safety instructions, and minimal technical context needed for routing, abuse prevention, and delivery.
- Pet or child/family profile context only where the user has lawfully entered such data and the feature requires it.

The operational principle is minimization: send no more data than reasonably needed for the function. Users must avoid entering unnecessary sensitive data in prompts or notes.

8.3 Training, Reuse, and Retention by AI/LLM Providers

Service objective: DashaMap is not designed to use users personal data as generalized third-party model training data. The practical ability to exclude provider training/reuse depends on the active provider, configuration, and contract. DashaMap favors, where available and reasonable, protective configurations that limit data use to service delivery and reduce unnecessary retention or training.

Some providers may retain prompts, outputs, metadata, or logs for limited periods for security, quality, anti-abuse, legal compliance, or operational reasons. Absolute zero retention cannot be guaranteed in every configuration.

8.4 Automated Decision-Making and Profiling - Art. 22 GDPR

DashaMap generates symbolic, interpretive, educational, and reflective outputs. It is not designed to make decisions based solely on automated processing that produce legal effects or similarly significant effects on a person. The Service must not be used as the sole basis for medical, psychological, veterinary, legal, financial, employment, credit, insurance, child welfare, or other high-impact decisions. Outputs remain subject to human review and user responsibility.

9. Cookies and Similar Technologies

DashaMap's preference panel provides necessary technologies and one optional analytics choice. Necessary technologies cannot be disabled through that panel where they are required for the requested service or to apply privacy choices. Users can refuse optional analytics, accept it, or save their analytics selection, and reopen preferences through the footer. There is no separate active marketing switch in this configuration. Promotional-email choices remain separate.

Acceptance and refusal are valid for 365 days from the saved choice timestamp. Ordinary visits do not renew that period. The choice applies to the browser/site storage concerned, not automatically to every device or account. Expiry is checked during an open page, after suspended-page resumption and when changes are received from another tab. Browser storage may retain an expired record physically, but it does not authorise collection.

The first-party visitor cookie has a maximum age of 365 days from its latest permitted setting; the session cookie has a maximum age of 30 minutes. Their refresh does not extend the consent deadline. A server session with a missing or expired consent deadline cannot accept new first-party analytics events.

Withdrawal stops new optional browser collection and requests server revocation of the affected visitor identifiers. On successful processing, the server deletes the first-party analytics events and sessions linked to those identifiers and records the revocation before expiring the visitor/session cookies. A failed request is retried; a pending browser marker prevents premature reactivation. Subsequent events using revoked identifiers are blocked. This operation does not close an account, cancel a subscription, delete readings or alter payment and Sparks records. It does not delete provider-held Vercel reports or identify records belonging to other browsers whose identifiers are unavailable.

Analytics identifiers included in subscription, gift and one-shot checkout metadata are conditional on valid consent and identifier checks. Refusal does not prevent necessary payment, order, delivery or security processing. Optional source/referral measurement does not become necessary merely because it relates to a purchase.

The Cookie Policy provides the identifier inventory, provider distinctions, withdrawal details and storage durations. Vercel collection is subject to the optional browser-analytics choice, but the first-party revocation and cleanup database does not erase Vercel-held records.

10. Data Recipients and Roles

The Controller shares personal data only where necessary to provide the Service, operate features, comply with legal obligations, ensure security, prevent abuse, handle payments, deliver emails, support users, or defend rights.

10.1 Typical Categories of Recipients

- Authentication, database, and storage providers, such as Supabase or equivalents.
- Payment, billing, subscription, tax, invoice, and fraud-prevention providers, such as Stripe or equivalents.
- Hosting/CDN and application infrastructure providers, such as Vercel or equivalents.
- Email, notification, deliverability, and operational communication providers.
- AI/LLM providers, gateways, or aggregators used for AI-assisted features.
- Monitoring, logging, error tracking, analytics, and security tools.
- Professional advisors such as legal, tax, accounting, audit, compliance, or technical consultants where necessary.
- Public authorities, courts, payment networks, or regulators where required by law or valid process.

10.2 Roles of Recipients

Depending on the service/function, recipients may act as processors under Art. 28 GDPR, sub-processors, or independent controllers for their own purposes. For example, a payment provider may process data as a processor for checkout and as an independent controller for anti-fraud, compliance, tax, or regulatory obligations according to its own terms and applicable law.

10.3 No Sale of Personal Data

The Controller does not sell users personal data.

11. International / Extra-EEA Transfers

Because the Controller is a U.S. company and may use global providers, some processing may involve transfers of personal data outside the EEA and/or the UK. Where applicable and required, the Controller adopts appropriate transfer tools and safeguards, which may include Standard Contractual Clauses, UK transfer tools, adequacy mechanisms where available, transfer impact assessments where required, minimization, encryption in transit, access controls, and provider role assessment.

For AI/LLM, infrastructure, payment, email, monitoring, and security providers, processing regions and transfer tools may vary over time. Additional operational details may be included in the DPA, enterprise due- diligence materials, provider documentation, or annexes where available.

12. Retention Periods and Retention Criteria

The Controller keeps personal data only for the time necessary for the relevant purposes and legal obligations, considering the contractual relationship, security needs, legal/fiscal obligations, disputes, chargebacks, fraud prevention, account closure, deletion requests, and backup cycles.

12.1 Practical Rules

- Accounts and profiles/Souls: retained while the account is active and needed to provide the Service; after deletion, deleted or de-identified except where retention is required or permitted by law, security, fraud prevention, accounting, or dispute defense.
- Generated outputs, reports, PDFs, and user content: retained within the account or feature configuration while available, subject to plan limits, product settings, user deletion, shared-link expiration, technical changes, and legal retention exceptions.
- Gift and one-shot product records: retained as needed to provide delivery, claim, activation, support, refund/non-delivery handling, fraud prevention, accounting, and dispute defense.
- Payment and billing data: retained according to applicable fiscal/accounting/administrative obligations, with the applicable period determined by jurisdiction, document type and the Controller's obligations. This notice does not represent a single verified 5-10-year schedule for every record.
- Selected ordinary application logs become eligible for automatic deletion after 90 days. The rule also covers narrowly selected free-test and concierge technical failures without linked Sparks movements or protected delivery evidence. Selected failed-reading logs qualify only when a complete matching Sparks refund is verified and both the event and refund are older than 90 days. Incomplete refunds, inconsistent records, protected delivery evidence and cases outside these rules are excluded. The cleanup does not change the Sparks ledger, balances, purchases, readings or PDFs.
- Security and denied-access events, and paid-service, failure or refund evidence excluded from automatic deletion, are reviewed 12 months after the event. Records no longer necessary are deleted; necessary records are retained only for an identified support, security, dispute or applicable legal purpose. For an open incident or dispute, the reason, scope and next review date are recorded and necessity is reviewed every 90 days. Review is manual and does not imply automatic deletion at 12 months or indefinite renewal.
- The current Supabase Free plan does not include scheduled project backups. Temporary manual exports or troubleshooting copies containing personal data are removed when the intervention ends, with an ordinary maximum of 30 days from creation. A longer exception requires a documented purpose and review date. Source code without personal data is outside this rule. This is a manual procedure, not a claim of automatic provider deletion. If backup services are activated later, their scope, retention and restoration safeguards must be defined and disclosed before use.

12.2 Detailed Analytics and Monthly History

Detailed first-party events become eligible for deletion 12 calendar months after their event timestamp; sessions become eligible 12 calendar months after their start timestamp. Scheduled daily maintenance deletes eligible rows in bounded batches. Deletion follows successful processing after the threshold, rather than occurring at the exact second it is reached. Failures or backlogs require remediation. The threshold is not postponed until the end of the month.

Before deletion, the system can preserve monthly totals for visitors, sessions, page views, registrations, checkouts and purchases. Counts are rounded to the nearest five. A metric based on fewer than ten distinct visitor identifiers is withheld rather than shown as zero. The archive contains month/environment and those counts, without visitor, account or transaction identifiers, page paths, names or individual reading content. Access is restricted; displayed figures are read-only and are not an exact financial ledger.

Monthly statistical totals become eligible for scheduled deletion after 36 months measured from the original statistical month, not from the date of archiving. Minimal visitor-revocation entries become eligible after 365 days from their revocation timestamp, provided no linked detailed analytics events or sessions remain. Repeated withdrawal does not renew the original revocation date. Processing occurs in bounded daily batches; failures and backlogs require follow-up. Restricted access, rounding and suppression of small groups reduce detail but do not

by themselves establish irreversible anonymisation. These periods are operational choices, not universal statutory deadlines or authority to retain data after its lawful purpose ends.

12.3 Personal Readings and Other Records

The analytics cleanup does not delete Oracle or Sinfonia readings, generated PDFs, the personal archive, accounts, profiles, birth data, orders, invoices or payment records. The 12-month analytics rule therefore does not impose a 12-month expiry on access to personal readings. Access and retention of those separate records remain governed by their own purposes, account/product terms, deletion choices and applicable rights.

The same analytics job does not control Vercel reports, infrastructure logs, backups or email copies. Their retention must be determined separately. See Annex B for contact delivery-control records.

13. Security Measures

The Controller applies technical and organizational measures proportionate to the nature of the Service and the risks, including encryption in transit, logical access controls, least privilege, environment-based secrets management, tenant/profile segregation where applicable, logging, anomaly monitoring, anti-abuse controls, rate limiting, suspicious pattern detection, vulnerability management, hardening, and incident response processes.

No system is completely invulnerable. In the event of a personal data breach, the Controller will act in accordance with applicable law, including notification obligations where required.

14. Data Subject Rights

If you are in the EEA/UK or in another jurisdiction recognizing similar rights, you may exercise, within applicable limits and conditions, rights of access, rectification, erasure, restriction, portability, objection, withdrawal of consent, and complaint to the competent supervisory authority.

To exercise rights, send an email to info@globalmountain.group with subject "GDPR Request - DashaMap" or equivalent, indicating the account email and the request. For security reasons, the Controller may request reasonable identity verification. Where GDPR applies, the Controller normally responds within 1 month, subject to lawful extensions for complex or numerous requests.

15. Deletion Requests and Practical Effects

In the event of a valid erasure request, the Controller may close the account, delete or de-identify associated profiles/Souls and content, revoke Magic Links/shared resources, and remove identifying data from active systems, subject to technical propagation time and legal exceptions.

The Controller may retain data that is necessary for legal obligations, accounting, anti-fraud, payment disputes, chargebacks, security investigations, contractual recordkeeping, litigation defense, or temporary backup residues. Deletion may affect access to reports, PDFs, outputs, gifts, one-shot products, subscriptions, Credits/Sparks history, and support continuity.

15.1 Withdrawal and Erasure Are Distinct Operations

Withdrawal stops new optional browser collection and requests server revocation of the affected visitor identifiers. On successful processing, the server deletes the first-party analytics events and sessions linked to those identifiers and records the revocation before expiring the visitor/session cookies. A failed request is retried; a pending browser marker prevents premature reactivation. Subsequent events using revoked identifiers are blocked. This operation does not close an account, cancel a subscription, delete readings or alter payment and Sparks records. It does not delete provider-held Vercel reports or identify records belonging to other browsers whose identifiers are unavailable. Erasure obligations can require action earlier than the routine retention deadline; users need not submit a second request where erasure is already required after withdrawal.

A separate erasure request can concern specified data or the account as a whole. Its consequences must be assessed against the request's scope; a request about analytics must not automatically be treated as a request to delete purchased readings. Pseudonymisation is not erasure where the person remains identifiable.

16. Minors and Child Data

DashaMap is not intended for use directly by minors and is not designed to knowingly collect personal data from minors in violation of applicable law. If the Controller becomes aware of an account or data relating to a minor managed in violation of applicable rules, it may suspend or delete the account/data within the limits of law.

Certain features, such as Child Evolution Atlas or family profiles where available, may allow an adult user to enter data relating to a child or family member. The adult user remains responsible for having parental responsibility, guardianship, consent, authority, notice, or another valid lawful basis required by applicable law. The Service is not pediatric, psychological, educational, welfare, or medical advice and must not be used as a substitute for qualified professionals.

In the EEA, Article 8 GDPR provides specific rules on consent for information society services offered directly to children, with age thresholds that may vary by Member State. Parents/guardians may contact info@globalmountain.group with subject "Privacy - Minor/Child Data - DashaMap" for verification/removal requests.

17. Communications

17.1 Operational Communications

The Controller may send communications necessary for the provision, security, billing, and administration of the Service, including receipts, billing notices, account notices, security alerts, maintenance notices, policy notices, gift delivery/claim emails, one-shot delivery emails, support messages, application status messages, and partner/referral operational notices.

17.2 Whispers and Service Notifications

Whispers and similar notifications are linked to Service settings and user preferences. Users may manage them through available settings where provided. Depending on the nature of the notification and applicable law, the legal basis may be contract, legitimate interest, or consent.

17.3 Marketing Communications

Marketing or promotional communications require the legal basis and communication permissions applicable to the specific message. Acceptance of analytics cookies is not consent to promotional email. Any separate promotional-email choice must be assessed and recorded for that purpose. Unsubscribe or opt-out mechanisms must be available as required, without blocking necessary transactional messages.

18. Automated Anti-Abuse, Fraud Prevention, and Security Signals

To protect the Service, users, payment flows, gifts, referrals, partner programs, Certified Astrologers flows, shared links, and technical supply chain, the Controller may process technical signals and usage patterns such as IP address, user agent, rate patterns, access anomalies, device/session indicators, payment signals, duplicate- click patterns, anti-bot indicators, and security events.

These controls serve security and integrity purposes and are not intended to produce legal or similarly significant automated decisions within the meaning of Article 22 GDPR. Some suspicious events may trigger temporary technical limitations, verification requests, throttling, blocks, or manual review pending verification, as provided by the ToS/AUP and applicable law.

19. Processing on Behalf of Business / White-Label Customers

When DashaMap is used by business, white-label, enterprise, Partner/Dealer, professional, or client-facing customers for profiles or reports relating to third parties, roles and responsibilities may vary depending on the actual configuration and contractual arrangements. In some cases, the business customer may act as controller and GLOBAL MOUNTAIN GROUP LLC may act as processor for specific processing activities, governed by a DPA or written terms.

The business customer that collects, enters, determines, or instructs processing of third-party data remains responsible for lawful basis, notices, consents, confidentiality, downstream disclaimers, data minimization, and compliance toward the relevant data subjects unless otherwise agreed in writing and within the limits of law.

20. Certified Astrologers, Partner/Dealer, Referral, Coupon, and Application Flows

Where DashaMap operates Certified Astrologers, Partner/Dealer, referral, coupon, ambassador, or similar programs, the Controller may process application data, approval/refusal records, public profile information submitted for listing, payment/activation status, referral codes, coupon usage, commission or reward data, fraud checks, internal review notes, and compliance records.

Public publication of astrologer or partner information occurs only where the relevant program and accepted terms provide for publication or where the user/applicant submits information for that purpose. Program access may be approved, refused, suspended, revoked, or limited in accordance with applicable terms and law.

Referral, coupon, commission, and partner records may be retained as needed for anti-fraud, payment verification, payout calculation, dispute handling, tax/accounting, compliance, and enforcement of program terms.

21. Alignment with ToS, AUP, Cookie Policy, DPA, AI Notice, and Disclaimer

This Privacy Policy shall be read together with the Terms of Service, Acceptable Use Policy, Cookie Policy, AI Transparency & Compliance Notice, Astrological Disclaimer, Refund / Billing / Subscription / Credits Policy, and, where applicable, the Data Processing Addendum and any written business agreement.

In the event of apparent conflict: the Cookie Policy governs cookies and similar technologies; the ToS governs contractual matters, accounts, subscriptions, billing, credits, suspension, termination, and disputes; the AUP governs prohibited conduct, abuse, security, scraping, and enforcement; the AI Notice governs AI transparency, AI limitations, routing, and governance; the Astrological Disclaimer governs symbolic/edutainment nature, non-professional-advice status, no-reliance, and related liability disclaimers; the DPA governs processor/customer role allocation and documented instructions where applicable; and this Privacy Policy governs personal data categories, legal bases, transparency, retention, transfers, rights, and privacy matters. Mandatory, non-derogable rights remain unaffected.

22. Changes to this Privacy Policy

The Controller may update this Policy for legal, regulatory, technical, security, privacy, product, provider, billing, business, or operational reasons. The updated version will be published in the Site/Service or Legal Center with an updated version, Last Updated date, and/or Effective Date. Where required by law or where changes are material, the Controller may provide additional notice through email, dashboard, in-app notice, or other reasonable means. Renewed consent will be requested where legally required.

23. Language and Controlling Version

This English version is the controlling version of this Privacy Policy unless a different controlling version is expressly designated in a signed written agreement with DashaMap. Translations are provided for convenience only. In the event of inconsistency, ambiguity, or conflict between language versions, the English controlling version prevails, subject to mandatory applicable law.

24. Contact Details

GLOBAL MOUNTAIN GROUP LLC

30 N Gould St #39973, Sheridan, WY 82801, United States.

Company ID: 2023-001208525 Email: info@globalmountain.group

Website: www.globalmountain.group

ANNEX A - SUB-PROCESSOR LIST (CATEGORIES, ROLES, AND TRANSPARENCY)

A.1 Purpose

This Annex provides operational transparency on categories of third-party providers that may process personal data within DashaMap, the typical purposes of processing, and possible roles. The list is category- based because the technical configuration may evolve. A more detailed named list may be provided for enterprise due diligence where appropriate and subject to confidentiality and security constraints.

A.2 Provider Categories

- Authentication, database, and storage providers: account authentication, profile/workspace storage, data persistence, outputs/files, and support functions. Typical data: email/account ID, profile/birth data, user-entered content, outputs, and technical logs. Typical role: processor/sub-processor depending on configuration.
- Payment and subscription providers: checkout, recurring subscriptions, one-shot purchases, gifts, add-ons, invoices, receipts, disputes, taxes, and fraud prevention. Typical data: billing data, transaction identifiers, payment status, anti-fraud/compliance signals. Role may include processor and independent controller functions.
- Hosting/CDN/infrastructure providers: site/app delivery, hosting, caching, performance, resilience, and security. Typical data: IP, user agent, HTTP requests, technical logs, and telemetry. Typical role: processor/sub-processor.
- Email, notification, and deliverability providers: operational emails, receipts, Whispers, gift delivery, one- shot delivery, security messages, and deliverability management. Typical data: email address, message metadata, sending preferences, delivery/failure logs, and message content where necessary. Typical role: processor.
- AI/LLM providers and gateways: generation or assistance in generating interpretive content, explanations, summaries, report texts, and related AI functions. Typical data: minimized prompts, portions of birth data or derived results, user question/input, style/templates, and security context. Role: generally processor for service delivery; provider-specific security/legal functions may differ.
- Monitoring, logging, error tracking, analytics, and security tools: incident detection, abuse prevention, debugging, audit, reliability, and security. Typical data: technical logs, event IDs, session indicators, IP, stack traces where applicable, and security events. Typical role: processor.
- Professional advisors and consultants: legal, tax, accounting, audit, compliance, and extraordinary operational support where necessary. Data is limited to what is necessary for the assignment. Role depends on the assignment and applicable law.

A.2.1 Named Services Identified in the Current Integration

Supabase provides database/authentication infrastructure; Stripe supports checkout and payments; Vercel provides hosting and optional Web Analytics; Resend delivers email. Hostinger hosts the operational mailbox, including info@dashamap.com and its admin/support aliases. Operational email copies are also received in Gmail. Provider-specific contractual entities, roles, regions, sub-processors and transfer safeguards follow the active agreements and configuration; naming a provider does not establish verification of all those matters.

The provider categories above remain relevant to other features, including AI. This notice does not invent a current AI model/provider inventory or claim verified zero retention. The active recipient and transfer information must be available under applicable transparency obligations; security or commercial confidentiality does not remove those obligations.

A.3 Provider Updates

The Controller may add, replace, or remove providers for technical, security, legal, product, reliability, compliance, or operational reasons. Material changes relevant to privacy rights or contractual commitments may be notified according to the ToS/DPA and applicable law.

A.4 Named List Requests

Data subjects may request recipient information and applicable transfer safeguards through the privacy contact. The Controller will provide information required by applicable law; this right is not limited to enterprise customers. Enterprise customers may also request the current sub-processor information required under their DPA. Any confidentiality restriction must respect mandatory transparency and access rights.

ANNEX B - DATA RETENTION SCHEDULE, DELETION, AND BACKUPS

B.1 Principles

- Retain data only for as long as necessary for the stated purposes.
- Delete, de-identify, or anonymize data where possible after the purpose ends, unless further retention is required or permitted.
- Apply differentiated retention periods by data category and risk.
- Retain minimum evidence for security, fraud prevention, billing, and dispute defense within lawful limits.

B.2 Practical Retention Rules by Category

- Account and profile data: retained while the account is active and needed for the Service; deleted/de-identified after closure or valid erasure, subject to exceptions.
- User content and generated outputs: retained according to account, feature, plan, and product configuration; some outputs may be regenerated, replaced, or unavailable in the same form after technical updates.
- Shared PDFs and Magic Links: may expire, be revoked, be watermarked, or be restricted for security and minimization.
- Payment and billing records: retained according to fiscal/accounting obligations and payment/dispute needs.
- Selected ordinary application logs become eligible for automatic deletion after 90 days. The rule also covers narrowly selected free-test and concierge technical failures without linked Sparks movements or protected delivery evidence. Selected failed-reading logs qualify only when a complete matching Sparks refund is verified and both the event and refund are older than 90 days. Incomplete refunds, inconsistent records, protected delivery evidence and cases outside these rules are excluded. The cleanup does not change the Sparks ledger, balances, purchases, readings or PDFs.
- Security and denied-access events, and paid-service, failure or refund evidence excluded from automatic deletion, are reviewed 12 months after the event. Records no longer necessary are deleted; necessary records are retained only for an identified support, security, dispute or applicable legal purpose. For an open incident or dispute, the reason, scope and next review date are recorded and necessity is reviewed every 90 days. Review is manual and does not imply automatic deletion at 12 months or indefinite renewal.
- The current Supabase Free plan does not include scheduled project backups. Temporary manual exports or troubleshooting copies containing personal data are removed when the intervention ends, with an ordinary maximum of 30 days from creation. A longer exception requires a documented purpose and review date. Source code without personal data is outside this rule. This is a manual procedure, not a claim of automatic provider deletion. If backup services are activated later, their scope, retention and restoration safeguards must be defined and disclosed before use.

B.2.1 Analytics Retention

The 12-calendar-month event/session threshold and daily batch processing are described in Section 12.2. Monthly totals have a 36-month period measured from the original statistical month; minimal revocation entries have a 365-day threshold subject to absence of linked details. Withdrawal erases the linked first-party events and sessions on successful server processing. These schedules do not control provider-held data.

B.2.2 Contact Delivery Controls and Email Copies

The contact-delivery claim operation removes request-control rows older than two days and rate-limit rows older than two hours when it runs. This is cleanup triggered by incoming claims, not a guaranteed timed deletion service: records can remain longer if no later claim occurs. The request-control table holds identifiers, keyed hashes, status and technical times; the rate-limit table holds keyed hashes and counters/times.

Ordinary support correspondence is reviewed monthly and deleted when more than 12 months have elapsed since closure of the request, unless a documented dispute, legal obligation or continuing support need requires a limited exception. The procedure covers the support mailbox, sent and archive folders, and operational Gmail copies. It is manual, not a mailbox timer; messages placed in the trash may remain there for up to 30 days before permanent removal. Billing and dispute correspondence is assessed under its own justified retention rules. This procedure does not delete copies held separately by the delivery provider.

Support email copies follow the monthly manual review described above. Application and professional-program records remain subject to their separate continuing purposes and applicable rights; they are not all ordinary support messages.

B.3 Deletion and Residual Limitations

Deletion may require technical propagation time. Any authorised residual copy remains subject to restricted access and a documented removal deadline; restoring a copy must not undo an applicable erasure without reapplying that erasure. A possible residual copy is not a blanket reason to postpone deletion from active systems. De-identification or anonymisation may be used only where compatible with the purpose and applicable law.

B.4 Review and Updates

This Annex may be updated to reflect architecture, providers, product flows, legal obligations, or security practices.

ANNEX C - EXTRA-EEA TRANSFERS, SAFEGUARDS, AND TRANSPARENCY

C.1 Scope

This Annex summarizes how the Controller addresses transfers outside the EEA and/or UK, considering that the Controller is a U.S. company and may use global providers.

C.2 When Transfers May Occur

- The Controller or providers process data from infrastructure located outside the EEA/UK.
- Support, security, monitoring, payment, email, AI/LLM, or operational functions involve personnel or systems in third countries.
- Global providers use sub-processors, regions, gateways, or failover infrastructure outside the EEA/UK.

C.3 Transfer Tools and Safeguards

- European Commission Standard Contractual Clauses or equivalent transfer tools where required.
- UK transfer tools where applicable.
- Adequacy mechanisms where available.
- Additional contractual, technical, and organizational measures, including minimization, encryption, access controls, and provider assessments.
- Transfer Impact Assessments or equivalent assessments where required.

C.4 AI/LLM and Zero Retention Note

For AI/LLM functions, the Controller seeks settings/contracts that reduce retention and avoid generalized training use of user data where available. Some providers may impose minimum retention for security, anti- abuse, or legal compliance, so absolute zero retention cannot be guaranteed in every configuration.

ANNEX D - SUMMARY OF TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

D.1 Purpose and Scope

This Annex provides a non-exhaustive summary of categories of technical and organizational measures adopted by the Controller. Measures evolve over time and not all implementation details are publicly disclosed for security reasons.

D.2 Example Categories of Measures

- Transmission security: HTTPS/TLS and protected communications between client, application, and providers.
- Access management: least privilege, logical access controls, account/role segregation, and tenant/profile segregation where applicable.
- Secrets and credentials: environment-based secret management and restricted access to production credentials.
- Application/infrastructure security: rate limiting, anti-abuse/anti-bot controls, suspicious pattern detection, monitoring, logging, patching, and vulnerability management.
- Operational resilience: error monitoring, troubleshooting workflows, incident response, backup, recovery, and disaster-recovery procedures proportionate to the configuration.
- Governance: need-to-know access, review of controls, provider coordination, and DPA/security obligations where applicable.

D.3 Breach Note

No system is invulnerable. In the event of a personal data breach, the Controller will follow applicable incident handling and notification obligations.

ANNEX E - DSAR PROCEDURE AND IDENTITY VERIFICATION

E.1 How to Submit a Request

Send an email to info@globalmountain.group with subject "GDPR Request - DashaMap" or equivalent, indicating account email, request type, context, and any information useful to locate the relevant data.

E.2 Identity Verification

Before executing a request, the Controller may require reasonable verification to ensure that the request comes from the data subject or an authorized person. Verification may include confirmation from the account email, minimum additional information, or enhanced confirmation for sensitive requests such as erasure, portability, or account takeover risk.

E.3 Timing and Handling

Where GDPR applies, the Controller responds without undue delay and within one month of receipt of the request. Where necessary because of complexity or number, the period may be extended by two further months; the user must be informed within the first month of the extension and reasons. Any identity-verification step must be proportionate and handled under the applicable deadline rules. If no action is taken, the Controller explains the reasons and the available complaint and judicial-remedy options within the applicable deadline.

E.4 Practical Effects of Erasure

Valid erasure may result in account closure, deletion or de-identification of profiles and contents, revocation of shared resources, and removal from active systems, except where retention is necessary for legal obligations, fraud prevention, disputes, litigation defense, accounting, security, or temporary backup residues.

E.5 Requests by Parents/Guardians

If a request concerns data of a minor, the Controller may request reasonable proof of parental responsibility/guardianship and minimum information necessary to identify the relevant account or data.

Legal references for the updated consent, retention and representation provisions: Regulation (EU) 2016/679, Articles 5, 7, 12-17 and 27 (https://eur-lex.europa.eu/eli/reg/2016/679/oj); EDPB Guidelines 05/2020 on consent

and Guidelines 3/2018 on territorial scope, available at https://www.edpb.europa.eu; ICO guidance on representatives, available at https://ico.org.uk. These references do not constitute certification or replace the Controller's implementation obligations.

END OF PRIVACY POLICY