PRIVACY POLICY (GDPR) - DASHAMAP

Full English Controlling Version

Version: 1.1
Last Updated: June 21, 2026
Effective Date: June 21, 2026

Table of Contents

PRIVACY POLICY (GDPR) - DASHAMAP

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. If you do not accept this Policy, you must not use the Service.

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 #47047, Sheridan, Wyoming 82801-6317, U.S.A.

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.

EU / UK representative: GLOBAL MOUNTAIN GROUP LLC is established in the United States. The applicability of Article 27 GDPR / UK GDPR representative requirements depends on the actual processing, territorial scope, targeting/monitoring analysis, and available exemptions. If and to the extent a representative is legally required or appointed, the relevant details will be published in this section or in the Legal Center. Until then, EU/UK privacy requests may be submitted directly to the privacy contact above. This does not limit any mandatory rights of data subjects.

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.

4.6 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.

4.8 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

Where enabled and lawful, DashaMap may process aggregate, pseudonymized, or minimized data to understand usage, performance, errors, latency, feature quality, reliability, abuse patterns, and infrastructure capacity. Non-necessary analytics and marketing technologies are governed by the Cookie Policy and applicable consent mechanisms.

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.
- Aggregate or technical analyses to improve performance and reliability, subject to minimization and balancing.

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 processing carried out before withdrawal.

7.5 Special Categories - Art. 9 GDPR

DashaMap is not designed to request special categories of personal data such as health data, religious beliefs, sexual orientation, political opinions, or criminal data. Users are asked not to enter such data unless strictly necessary, lawful, and supported by an appropriate legal basis under their own responsibility. Birth data is treated as highly identifying and operationally sensitive even where it is not an Art. 9 special category by itself.

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 may use cookies and similar technologies for technical, functional, analytics, and, if activated, marketing purposes. Full details are described in the Cookie Policy and any available banner/CMP or cookie settings.

- Necessary/technical: session, login, locale, security, CSRF/anti-abuse, and service stability. Legal basis: contract and/or legitimate interest.
- Functional: UI preferences, display modes, and optional settings. Legal basis: consent where required, otherwise legitimate interest.
- Analytics: performance and usage measurement in aggregate or pseudonymized form where enabled. Legal basis: consent where required.

- Marketing/referral/campaign: campaign, referral, and conversion tracking where enabled and lawful. Legal basis: consent where required.

The Cookie Policy must reflect the actual technical implementation. If a preference center, banner, or cookie settings tool is available, users may manage preferences through it and/or browser settings, subject to technical limitations.

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, often 5-10 years depending on jurisdiction and document type.
- Technical, security, anti-abuse, and fraud logs: generally retained for limited periods, for example 30 days to 12 months depending on the log type, with possible extension for incidents, disputes, investigations, fraud, or legal claims.
- Support, application, Partner/Dealer, and Certified Astrologer records: retained for the time needed to handle the request, maintain program integrity, support auditability, and defend against disputes, subject to legal obligations and deletion rights.
- Backups: residual copies may remain for a limited technical period and are progressively overwritten according to backup and disaster-recovery cycles.

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.

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 are sent on the legal basis required by applicable law, typically consent where necessary. Unsubscribe or opt-out options are provided where required.

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 #47047, Sheridan, Wyoming 82801-6317, U.S.A.

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.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

Upon reasonable and motivated enterprise due-diligence request, the Controller may provide a current named list of active providers, categories of processing, and main processing regions/countries where available, compatible with confidentiality obligations, security needs, and contractual restrictions.

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.
- Technical and security logs: retained for limited periods, extendable for incidents, fraud investigations, abuse, disputes, or legal claims.
- Support/application/program data: retained as needed for request handling, auditability, program integrity, disputes, and legal obligations.
- Backups: residual copies may remain temporarily and are overwritten according to backup and disaster-recovery cycles.

B.3 Deletion and Residual Limitations

Deletion may require technical propagation time. Data in backups may remain temporarily but is not ordinarily accessible in production. De-identification or anonymization may be used where compatible with law, security, audit, or statistical purposes.

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 normally within 1 month of receiving a valid request. The deadline may be extended where permitted by law for complex or numerous requests. If the request cannot be granted in whole or in part, the Controller will provide a reasoned response within applicable legal limits.

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.

END OF PRIVACY POLICY