PRIVACY POLICY (GDPR) – DASHAMAP

Table of Contents

Full English controlling version

Last updated: February 22, 2026

Effective date: February 22, 2026

This Privacy Policy transparently describes how DashaMap processes personal data, including birth data (date/time/place) necessary for calculations and interpretive content, as well as how it uses third-party providers (e.g., for authentication, infrastructure, payments, email, monitoring, and AI/LLM). If you do not accept the rules described here, we ask that you do not use the Service.

This notice is drafted taking into account, where applicable, Regulation (EU) 2016/679 (GDPR), national implementing rules, rules on cookies/similar technologies and electronic communications, consumer rules, and cybersecurity rules. References to GDPR articles are for operational transparency purposes and do not limit any additional obligations provided by applicable law.

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
- EIN: 61-2074460
- General email / Privacy contact: info@globalmountain.group
- Website: www.globalmountain.group

Recommended email subject for privacy requests: "Privacy - 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.
- EU / UK representative (Art. 27 GDPR / UK GDPR): if and to the extent that the obligation applies based on actual operations toward data subjects in the EEA or the United Kingdom and no exemption applies, the Controller will appoint a representative and publish the relevant details here. Until then, the privacy contacts remain those indicated above.

2. Scope of application

This Policy applies to:

- DashaMap website and application

Authentication areas, plans/subscriptions, workspace/sanctuary, oracles, PDF exports, Magic Links, referrals, and API functionalities (if active)

- Email communications and notifications connected to the Service (including "Whispers")
- Business / white-label / client portal functions, if activated

Support interactions and operational or privacy requests

In particular, the Policy describes the information required by Articles 12-14 GDPR, where applicable, using language that is as clear and operational as possible.

3. Essential definitions

- Service: the DashaMap platform and related functionalities (site/app, accounts, workspace, generations, exports, shareable links, plans, add-ons).
- User: natural person using the Service; includes individual users, authorized users of business customers, and invited persons.
- Business / white-label customer: professional entity using DashaMap for its own team or toward end customers, with or without brand customization.
- Souls / Profiles: profiles created in the Service, including those relating to third parties, containing birth data and other elements entered by the user.
- Output: content generated or reworked by the Service (texts, timelines, reports, PDFs, notifications, summaries, interpretations).
- Magic Link / shareable link: URL generated by the Service for access to or sharing of content with possible expiration/revocation.
- Third-party suppliers / providers: technical or commercial entities that process data on behalf of the Controller or, in some cases, as independent controllers for their own purposes.

4. Categories of processed data (what we collect)

4.1 Account and identification data

- Email

First name, last name, or nickname/display name (if entered)

- Language/locale, profile preferences, settings
- User ID / account ID and technical metadata linked to the account
- Credentials: authentication management may be delegated to providers (e.g., Supabase Auth); the Controller should not see passwords in plain text

Clarification on nickname / pseudonym:

For ordinary use of the Service, it is not always necessary to use your real legal name as the visible profile name

It is possible to use a nickname/display name/pseudonym, provided it does not violate the law, third-party rights, trademarks, others' identities, anti-abuse policies, or Service rules

The displayed name may not coincide with the name used for billing/payment

It remains the user's responsibility not to use deceptive names, not to impersonate third parties, and not to use others' data without legitimate title

Clarification on real data for payments, billing, and compliance:

For payments, billing, receipts, disputes, anti-fraud checks, or fiscal/legal obligations, the payment provider and/or the Controller may require real and correct identifying and billing data, to the extent necessary

In the event of false, incomplete, or unverifiable billing data, payment may be refused, suspended, or canceled and/or access to the Service may be limited, within the limits of law and the ToS

4.2 Birth data and profiles ("Souls")

This data constitutes the operational core of the Service.

Date of birth

Time of birth (if provided)

Place of birth (city/country and, where necessary, derived coordinates or time zone)

Profile elements linked to calculation or personalization (e.g., goals, tags, preferences)

- Notes, diary, memos, text entered by the user

Third-party data entered by the user:

If you enter data relating to third parties (e.g., partners, family members, collaborators, or other persons), you declare that you have a legal basis/legitimate title (consent, authorization, mandate, or another valid basis under applicable law)

Do not use the Service to process third-party data in an unlawful, invasive manner or contrary to privacy laws

4.3 Usage data and generated content

Actions and requests performed in the Service (e.g., activations, report generations, access to sections)

Content entered by the user (texts, questions, notes, diary, completed fields)

Outputs generated by the Service (texts, timelines, interpretations, reports, notifications)

Plan status, quotas, consumption/credits, and functional limits

Outputs may contain symbolic references and/or summaries of entered data. If linked to an account or an identifiable profile, outputs are treated as personal data.

4.4 Payment and billing data (payment provider, e.g., Stripe)

Subscription status, active plan, renewals, upgrades/downgrades

Transaction history, transaction identifiers, customer ID, subscription ID

- Receipts, invoices, and necessary administrative/fiscal data

Billing data (first/last name or company name, address, fiscal data if required)

Payment outcome and anti-fraud/compliance signals from the provider

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

Access and usage logs

Security events, application errors, stack traces (where applicable)

- Anti-fraud/anti-abuse signals, rate limiting, access patterns

Cookies and similar technologies (see the Cookie Policy)

4.6 Communication and notification data ("Whispers")

Communication and notification preferences (e.g., configured frequency/modes)

Data necessary to send operational emails/notifications

- Delivery/failure logs for deliverability, spam prevention, and support

4.7 Support and assistance data

Content of support requests/tickets

Attachments or screenshots voluntarily sent

Support conversation history

Troubleshooting results and access restoration

4.8 Data we ask you NOT to enter (practical minimization)

Unless expressly requested by a specific function, we ask you not to enter unnecessary or particularly sensitive data in free-text fields, for example: health details, document numbers, credentials, OTP codes, seed phrases, complete financial data, data of third-party minors without title.

If such data is entered voluntarily, it may be processed only to the extent necessary to provide the Service, provide assistance, manage security/compliance, or fulfill legal obligations.

5. Data sources (where data comes from)

Personal data may come from:

Directly from the user (account registration, profile completion, notes, questions, payments, support)

From actions and use of the Service (logs, events, use of functions, preferences)

From payment providers (transaction statuses, identifiers, outcomes, anti-fraud information within allowed limits)

From technical providers (hosting, monitoring, email deliverability, security)

From other users/business customers who enter third-party data into profiles (e.g., white-label or professional use), in which case the user entering the data remains responsible for the title to process

When data is not collected directly from the data subject (e.g., third-party data entered by a business customer), the information obligations toward data subjects remain with the party that determines that processing and enters the data, unless a different legal/contractual arrangement applies and within the limits of law.

6. Purposes of processing (why we process data)

6.1 Provision of the Service and core functionalities

Creation and management of accounts

Creation and management of profiles/Souls

Calculation of timelines, cycles, historical memories, and related content

Generation of outputs, reports, exports (including PDF), and Magic Link management

Personalization of user settings and preferences

6.2 Subscriptions, billing, and credits/quotas management

Plan activation, renewals, upgrades/downgrades, add-ons, and gifts (if available)

Consumption measurement and application of limits (e.g., generations, PDF, export, staff accounts, API)

- Billing, receipts, and administrative obligations

Payment fraud prevention and dispute/chargeback management

6.3 Security, abuse prevention, and platform integrity

Rate limiting, anti-scraping, detection of anomalous access and abuse patterns

Audit logs, error monitoring, incident management, and security

- IP and content protection (watermarks, expiring links, revocations, restrictions)

Verification and mitigation of suspicious, fraudulent activities or activities in violation of ToS/AUP

6.4 Support and assistance

Response to tickets, operational requests, and privacy requests

Access restoration, troubleshooting, and technical communications

Operational communications on account, security, payments, maintenance

6.5 Product improvement, analytics, and reliability (if enabled)

Aggregate or pseudonymized statistics to understand usage and performance

Improvement of UX, reliability, service quality, and infrastructure capacity

Analysis of errors, response times, stability, and security

Where possible, the Controller favors minimization, aggregation, or pseudonymization. Analyses are aimed at product growth and security, not at undue surveillance of users.

6.6 Legal compliance and defense in case of disputes

- Fiscal, accounting, and administrative obligations
- Complaint, dispute, chargeback, and litigation management

Response to legitimate requests from authorities

Protection of the Controller and third parties in case of abuse, fraud, or unlawful use of the Service

7. Legal bases for processing (Art. 6 GDPR)

Depending on the purpose, the Controller uses one or more of the following legal bases (where GDPR applies):

7.1 Performance of a contract or pre-contractual measures (Art. 6(1)(b) GDPR)

Creation and management of accounts

Provision of requested functionalities (calculations, reports, exports, Magic Links, workspace)

Management of plans, subscriptions, credits/quotas, and technical support connected to the Service

Essential operational communications for the service (security, payment, maintenance)

7.2 Legal obligation (Art. 6(1)(c) GDPR)

- Fiscal, accounting, and administrative obligations

Responses to valid orders or legitimate requests from authorities

Mandatory retention required by law

7.3 Legitimate interest (Art. 6(1)(f) GDPR)

- Security, fraud/abuse prevention, anti-scraping, infrastructure protection, and technological supply chain protection

Error monitoring, resilience, operational continuity, uptime, and hardening

Protection of intellectual property, content, and defense in court

Aggregate or technical analyses to improve performance and quality of the Service

The Controller applies a balancing test and minimization, access control, and proportionality measures to reduce the impact on data subjects.

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

- Non-necessary cookies and technologies (analytics/marketing), where required

Marketing and promotional communications, where not permitted on another basis

Optional functionalities for which the law requires consent

Consent may be withdrawn at any time without affecting the lawfulness of processing carried out before withdrawal.

7.5 Special categories of data (Art. 9 GDPR) - clarification

DashaMap is not designed to request special categories of personal data (e.g., health, religion, sexual orientation, political opinions). If such data is voluntarily entered by the user in free-text fields, processing will occur only to the extent technically/operationally necessary and according to applicable legal bases, it being understood that the user is invited not to enter them unless strictly necessary.

Date, time, and place of birth normally do not fall within special categories under Art. 9 GDPR, but may be highly identifying and operationally sensitive. For this reason, the Controller treats them as data of high operational sensitivity (greater minimization, access controls, and security measures).

8. AI/LLM: use of AI, data sent, and limits

8.1 What AI does in DashaMap

Generates or assists the generation of interpretive and narrative content

Produces summaries, explanations, suggestions, and report texts

May use context entered by the user (e.g., questions, notes, tags) to formulate responses

For further details on AI governance, limits, no-reliance, and compliance, please also refer to the AI Transparency & Compliance Notice.

8.2 What data may be included in prompts

To provide the AI/LLM function, the Controller may send to the AI/LLM provider only the data necessary (need-to-know principle), for example:

Portions of birth data or derived calculation results

Question text or user input

Profile elements (e.g., goals, tags) if useful to the response

- Style/template instructions (including white-label) and security context

The operational principle is to minimize the content sent, avoiding the sending of unnecessary data.

8.3 Training, data reuse, and retention on the AI/LLM provider side

Service objective: NOT to use users' data as generalized training data. Operationally, the actual ability to exclude training/reuse depends on the contractual and technical options of the AI/LLM provider active at that time.

- The Controller favors, where available and applicable, options/contracts that limit data use to mere service delivery and reduce or exclude training
- The Controller applies minimization and, where possible, pseudonymization/anonymization measures

Some providers may retain logs for limited periods for security, quality, anti-abuse, or compliance

Absolute zero retention cannot be guaranteed if the provider imposes minimum retention for security or legal obligations

8.4 Automated decisions and profiling (Art. 22 GDPR)

DashaMap generates content and symbolic profiles, but it is not designed to make decisions producing legal effects or similarly significant effects on the user. The Service must not be used as the sole basis for medical, legal, financial, employment, or equivalent decisions. Output is interpretive/symbolic and remains subject to the user's evaluation and responsibility.

9. Cookies and similar technologies (summary)

DashaMap uses cookies and similar technologies for technical, functional, analytics, and, if activated, marketing purposes. Full details (categories, providers, legal bases, consent management, duration, and register/changelog) are described in the Cookie Policy and CMP/banner tools.

Necessary/technical (always active): session, login, language/locale, security (CSRF/anti-abuse), service stability. Legal basis: contract and/or legitimate interest.

Functional (optional): UI preferences, modes, and settings. Legal basis: consent where required, otherwise legitimate interest.

Analytics (optional): performance/usage measurement in aggregate or pseudonymized form. Legal basis: consent where required.

Marketing (optional): campaign and conversion tracking. Legal basis: explicit consent, where applicable.

The user may manage cookie preferences via the banner/CMP and/or available settings.

10. Data recipients and roles (who receives the data)

The Controller shares personal data only when necessary to provide the Service, comply with legal obligations, ensure security, or defend its rights.

10.1 Typical categories of recipients

- Authentication, database, and storage providers (e.g., Supabase or equivalents)

Payment and billing providers (e.g., Stripe or equivalents)

- Hosting/CDN and application infrastructure (e.g., Vercel or equivalents)
- Email/notification and deliverability providers
- AI/LLM providers for generations and responses
- Monitoring, logging, error tracking, and security tools
- Consultants, professionals (legal/tax/accounting), and auditors, if necessary

Public authorities, where required by law or valid orders

10.2 Roles of recipients

Depending on the service/function, recipients may act as data processors under Art. 28 GDPR, sub-processors, or - for specific own purposes (e.g., anti-fraud/payment compliance) - as independent controllers.

For example, a payment provider may process part of the data as a processor for checkout and, for other activities (anti-fraud, its own regulatory obligations), as an independent controller according to its terms.

10.3 No sale of personal data

The Controller does not sell users' personal data.

11. Extra-EEA / international transfers

Because the Controller is a U.S. company and uses global providers, some processing may involve transfers of data outside the EEA (Arts. 44 et seq. GDPR), including transfers to countries that may not benefit from an adequacy decision.

When applicable, the Controller adopts appropriate measures and safeguards, including:

- Standard Contractual Clauses (SCC) or other recognized transfer tools
- Transfer Impact Assessment (TIA), when required

Minimization of transferred data

Encryption in transit and, where possible, at rest

Choice of EEA regions/hosting when available and compatible with the active configuration

Assessment of the provider's actual role (processor/independent controller) and the function performed

For more operational detail on transfers and safeguards, also see the Attachments and contractual privacy/DPA documentation, where applicable.

12. Retention periods and criteria

The Controller keeps data only for the time necessary for the purposes and legal obligations (storage limitation principle).

12.1 General retention criteria

Duration of the contractual relationship and account

Technical and security needs

- Legal/fiscal/administrative obligations
- Complaint, dispute, chargeback, and litigation defense management

Backup cycles and technical overwrite times

12.2 Practical rules (summary)

Accounts and profiles (Souls): for as long as the account remains active; in case of deletion, deletion or de-identification except for legal obligations or defense against disputes/fraud.

Payment and billing data: retained according to applicable fiscal/accounting obligations (often 5-10 years, varying by jurisdiction).

Technical and security logs: limited retention (typically 30 days - 12 months), with possible extension in case of investigations into incidents/fraud/disputes.

Generated outputs and reports: available in the active account according to plan/limits; PDFs and Magic Links may have expiration or revocation for security.

Backups: residual copies may remain for a limited technical time and are overwritten according to backup cycles.

13. Security measures (summary, Art. 32 GDPR)

- The Controller applies technical and organizational measures proportionate to the nature of the Service and the risks, including, for example:

Encryption in transit (HTTPS/TLS)

Access controls and logical segregation (e.g., RLS/segregation where applicable)

Principle of least privilege

- Secrets/API key management through dedicated systems/environment variables
- Logging, anomaly monitoring, rate limiting, anti-abuse protections

Vulnerability management, hardening, and incident response processes

Reviews and updates of controls according to service evolution and risk

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

14. Data subject rights (GDPR and similar laws)

If you are in the EEA/UK or in jurisdictions recognizing similar rights, you may exercise, within the limits and conditions of applicable law:

Right of access

Right to rectification

Right to erasure ("right to be forgotten")

Right to restriction of processing

Right to data portability (where applicable)

Right to object (where processing is based on legitimate interest)

Right to withdraw consent (for processing based on consent)

Right to lodge a complaint with the competent supervisory authority

How 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 in case of complex or numerous requests.

15. Erasure requests and practical effects

In the event of a valid erasure request, the Controller may, within the limits of law:

Close the account and remove identifying data

Delete associated profiles/Souls and contents

Retain only what is necessary for legal obligations, accounting, anti-fraud, dispute/litigation defense

Maintain temporary residual copies in backups until overwrite

Revoke or disable Magic Links / shared resources, where applicable

16. Minors

DashaMap is not intended for 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 the rules, it may suspend and delete the account/data within the limits of law.

In the EEA, Art. 8 GDPR provides specific rules on consent for information society services offered directly to minors (age threshold that may vary by Member State, usually between 13 and 16). Parents/guardians may contact info@globalmountain.group for verification/removal (subject: "Privacy - Minor/Child Data - DashaMap").

17. Communications (operational, Whispers, marketing)

17.1 Operational communications

The Controller may send communications necessary for the provision and security of the Service (e.g., receipts, billing notices, account notices, technical maintenance, suspicious access). Legal basis: contract and/or legitimate interest.

17.2 Whispers and service notifications

Whispers (and similar notifications) are linked to the Service and user settings/preferences. The user may manage them in the available settings. 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/opt-out options are made available where required.

18. Automated anti-abuse checks, fraud prevention, and security signals

To protect the Service, users, and technological supply chain, the Controller may process technical signals and usage patterns (e.g., IP, user agent, rate patterns, access anomalies, anti-bot signals, basic device/session indicators) to detect abuse, fraud, scraping, circumvention, or security incidents.

These controls serve security and integrity purposes and are not intended to produce legal or similarly significant automated decisions on the user within the meaning of Art. 22 GDPR. Nevertheless, some suspicious events may trigger temporary technical limitations (e.g., throttling, verification requests, temporary blocks) pending verification, as provided by ToS/AUP.

19. Data processing on behalf of business customers / white-label

When DashaMap is used by business customers/white-label customers for profiles or reports relating to third parties, roles and responsibilities may vary depending on the actual configuration and contractual arrangements (ToS, DPA, enterprise clauses).

In such cases, the business customer that enters or determines the processing of third-party data remains responsible for the title/legal basis, information obligations, and lawfulness of the processing toward the relevant data subjects, unless otherwise agreed in writing and within the limits of law.

The Controller may act as processor for the business customer for specific processing activities, as governed by the applicable DPA/contractual documents.

20. Alignment with the Terms of Service, AUP, Cookie Policy, DPA and AI Transparency & Compliance Notice

This Privacy Policy shall be read in conjunction with the Terms of Service ("ToS"), the Acceptable Use Policy ("AUP"), the Cookie Policy, the AI Transparency & Compliance Notice, and, where applicable, the Data Processing Addendum ("DPA"). In the event of any apparent conflict or interpretive discrepancy: (i) the Cookie Policy shall prevail with respect to cookies, tracking technologies, and consent management; (ii) the ToS shall prevail with respect to contractual matters (including plans, billing, suspension/termination, and disputes); (iii) the AUP shall prevail with respect to usage rules, security, anti-abuse measures, and enforcement; (iv) the AI Transparency & Compliance Notice shall apply as a supplementary transparency and governance document with respect to AI-assisted functionalities, limitations, and non-reliance principles, and shall not limit or replace this Privacy Policy with respect to personal data processing/privacy matters; (v) the DPA, where applicable, shall prevail with respect to processor/customer role allocation, documented instructions, and other data processing terms agreed for business/white-label relationships; and (vi) this Privacy Policy shall prevail with respect to personal data processing, categories of personal data, legal bases, transparency obligations, retention, transfers, data subject rights, and privacy-related matters. In all cases, mandatory, non-derogable rights under applicable law remain unaffected.

21. Changes to this Privacy Policy

The Controller may update this Policy for technical, legal, security, product evolution, or provider changes.

The updated version will be published on the Site/Service with "Last updated" and/or "Effective date".

Where required by law or if the changes are material, the Controller may also provide additional notice (e.g., email, in-app notice, dashboard alert).

Continued use of the Service after the effective date of the updated version implies acknowledgment of the changes, without prejudice to mandatory rights and any actions required by law (e.g., renewed consent where necessary).

22. Controlling version and language

Unless otherwise indicated in a specific published version, the English version may be designated as the controlling version of this Policy. Translations are provided for convenience/courtesy only and do not alter the legal meaning of the controlling version.

If no English controlling version has yet been published, this version remains the reference text until the official controlling version is published.

23. Contact details

- GLOBAL MOUNTAIN GROUP LLC
- Email: info@globalmountain.group
- Website: www.globalmountain.group
- Registered office: 30 N Gould St #47047, Sheridan, Wyoming 82801-6317 - U.S.A.

ATTACHMENT A

SUB-PROCESSOR LIST (CATEGORIES, ROLES AND TRANSPARENCY)

A.1 Purpose of the attachment

This Attachment provides operational transparency on the categories of third-party providers that may process personal data within DashaMap, the typical purposes of processing, and the possible roles (processor/sub-processor/independent controller, depending on the function).

The list is expressed by categories and examples because the technical configuration may evolve over time. Where contractually or legally required (e.g., enterprise due diligence), the Controller may provide a more detailed named list, subject to confidentiality and security constraints.

A.2 Categories of providers, purposes, data, and roles (summary)

1. 1) Authentication, database, and storage providers (e.g., Supabase or equivalents)

- Purposes: account authentication, profile and workspace storage, data persistence, storage of outputs/files, technical support functions.
- Data typically involved: email/account ID, profile/birth data, user-entered content, outputs associated with the account, technical logs/metadata.
- Typical role: data processor on behalf of the Controller (or sub-processor within the infrastructure chain), depending on configuration and contractual framework.

2. 2) Payment and subscription providers (e.g., Stripe or equivalents)

- Purposes: checkout, payment processing, recurring subscriptions, receipts/invoices, dispute and fraud-prevention management.
- Data typically involved: billing data, transaction identifiers, customer ID/subscription ID, payment status/outcomes, anti-fraud/compliance signals.
- Clarification: complete card data are typically processed by the payment provider and are not stored in full by the Controller.
- Role: may operate partly as processor and partly as independent controller for its own regulatory/anti-fraud obligations, according to the provider's terms and the function performed.

3. 3) Hosting / CDN / infrastructure providers (e.g., Vercel or equivalents)

- Purposes: site/app delivery, hosting, caching/CDN, performance, resilience, security.
- Data typically involved: IP, user agent, HTTP requests, technical logs, performance/error telemetry.
- Typical role: processor or infrastructure sub-processor, depending on the setup.

4. 4) Email, notification, and deliverability providers

- Purposes: operational emails, security messages, receipts, Whispers, notification sending, deliverability management, anti-spam controls.
- Data typically involved: email address, sending preferences, message metadata, delivery/failure logs, message content (where necessary).
- Typical role: data processor.

5. 5) AI/LLM providers (language model providers)

- Purposes: generation or assistance in generating interpretive content, explanations, summaries, report texts, and related AI functions.

Data potentially involved in prompts/requests: portions of birth data or derived results, user question/input, profile context (e.g., tags/goals), style instructions/templates, security context.

- Operational principle: minimization (need-to-know); the Controller seeks not to send more data than necessary.
- Training/retention note: the Controller favors "no training" / reduced retention settings where available, but the actual options depend on the active provider and contractual/technical setup.
- Role: generally processor for service delivery; for certain security/abuse/legal compliance functions the provider may qualify differently according to its terms and the concrete processing.

6. 6) Monitoring, logging, error tracking, and security tools

- Purposes: incident detection, abuse prevention, error debugging, audit, operational reliability, security monitoring.
- Data typically involved: technical logs, event IDs, session indicators, IP, stack traces (where applicable), security events.
- Typical role: data processor.

7. 7) Professional advisors and consultants (legal/tax/accounting/audit), where necessary

- Purposes: legal defense, compliance, accounting/tax obligations, audits, management of extraordinary operations or disputes.
- Data typically involved: only the data necessary for the professional assignment (principle of minimization/need-to-know).
- Role: autonomous professionals or data processors depending on the assignment and applicable law.

A.3 Provider updates and change management

The Controller may add, replace, or remove providers for technical, security, legal, or operational reasons.

In the event of material changes relevant to privacy rights or contractual commitments, the Controller may provide notice according to the ToS/DPA and applicable law.

Continued use of the Service after the effective date of an update implies acknowledgment, without prejudice to mandatory rights (including any rights of objection/termination where contractually or legally provided).

A.4 Request for named list (enterprise / due diligence)

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

ATTACHMENT B

DATA RETENTION SCHEDULE, DELETION AND BACKUP

B.1 Purpose and principles

This Attachment summarizes retention criteria and operational retention/deletion rules applied by the Controller, in accordance with the storage limitation principle and taking into account contractual, security, and legal needs.

General principles:

Retain data only for the time necessary for the purposes for which they are processed

- Delete, de-identify, or anonymize data where possible once the purpose ends, unless further retention is required/allowed

Apply differentiated retention periods by category of data and risk

Retain minimum evidence for security, fraud prevention, and dispute defense, within lawful limits

B.2 Practical retention rules by category

8. 1) Account and profile data (Souls)

- Standard retention: for as long as the account remains active and the data are necessary to provide the Service.
- Deletion/closure: in case of erasure request or closure, the Controller deletes or de-identifies account/profile data, except for data whose retention is required by law or necessary for defense against disputes/fraud.

9. 2) User-entered content and generated outputs (texts, timelines, reports)

- Retention: generally available in the active account within plan limits and according to the Service configuration.

Notes: some outputs may be regenerated, replaced, or no longer available in the same format due to technical updates, product changes, or function evolution.

Shared PDFs / Magic Links: may have expiration, revocation, or access restrictions for security and data minimization reasons.

10. 3) Payment and billing data

- Retention: according to applicable fiscal/accounting/administrative obligations (often 5-10 years, depending on jurisdiction and document type).
- Card data clarification: complete card data are generally processed and retained by the payment provider according to its rules and obligations, not by the Controller.

11. 4) Technical, security, and anti-abuse logs

- Retention: generally limited (e.g., 30 days to 12 months) depending on type of log, security purpose, and operational needs.
- Possible extension: in the event of incidents, fraud investigations, abuse, disputes, or legal claims, relevant logs may be retained longer for the time necessary for handling and defense.

12. 5) Support and assistance data

- Retention: for the time necessary to handle the request and, thereafter, for a reasonable period to ensure continuity of support, prove what was handled, and defend against disputes, subject to legal obligations.

13. 6) Backups

Residual copies of deleted data may remain in backup systems for a limited technical period and are progressively overwritten according to backup and disaster recovery cycles.

B.3 Deletion, de-identification, and residual limitations

Deletion may not be immediate in every system and may require technical propagation time.

In some cases, instead of full deletion, data may be de-identified/anonymized where this better serves security, audit, or statistical purposes and is compatible with the purposes and applicable law.

During the backup overwrite period, deleted data may not be ordinarily accessible in production, but may remain temporarily in backup media.

B.4 Review and updates

The Controller may update this Attachment to reflect changes in architecture, providers, legal obligations, or security practices. Material changes are managed in line with the Privacy Policy/ToS/DPA, where applicable.

ATTACHMENT C

EXTRA-EEA TRANSFERS, SAFEGUARDS, AND TRANSPARENCY

C.1 Scope

This Attachment summarizes how the Controller addresses transfers of personal data outside the EEA (and, where relevant, the UK), considering that the Controller is a U.S. company and may use global providers.

C.2 When transfers may occur

International transfers may occur, for example, when:

- The Controller or a provider processes data from infrastructure located outside the EEA
- Support, security, monitoring, or operational functions involve personnel/systems located in third countries
- AI/LLM, email, infrastructure, or payment providers process data in non-EEA regions

C.3 Transfer tools and safeguards (where required)

Where applicable and required by GDPR/UK GDPR, the Controller may use one or more of the following safeguards/tools:

- European Commission Standard Contractual Clauses (SCC)
- UK transfer tools (where applicable)

Additional contractual, technical, and organizational measures (e.g., minimization, encryption, access controls)

- Transfer Impact Assessment (TIA) or equivalent assessments, where required

Use of adequacy decisions, where available

C.4 Operational measures for risk reduction

In addition to legal transfer tools, the Controller applies or may apply operational measures such as:

Data minimization (sending to providers only the information necessary for the function)

Preference for EEA regions/hosting when available and compatible with the service configuration

Encryption in transit and, where possible, at rest

Access controls and logging

Evaluation of the provider's role and the concrete processing carried out

C.5 Note on AI/LLM providers, retention, and 'zero retention'

For AI/LLM functions, the Controller seeks settings/contracts that reduce retention and avoid generalized training use of users' data, where available. However, some providers may impose

minimum retention periods for security, anti-abuse, or legal compliance purposes. Therefore, absolute 'zero retention' cannot be guaranteed in every configuration.

C.6 Additional information

Data subjects may request general information on transfer safeguards via the contacts indicated in the Privacy Policy, without prejudice to confidentiality limits, security needs, and protection of the Controller's contractual arrangements.

ATTACHMENT D

SUMMARY OF TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES (TOMs)

D.1 Purpose and scope

This Attachment provides a summary (non-exhaustive) of the categories of technical and organizational security measures adopted by the Controller, proportionate to the nature of the Service and processed data.

Security measures evolve over time for technical, operational, and threat-response reasons. For security reasons, this Attachment does not describe all implementation details.

D.2 Example categories of measures

14. 1) Transmission and communication security

Encryption in transit (HTTPS/TLS)

Protection of communications between client, application, and providers

15. 2) Access management and authorization

Logical access controls and least privilege principle

Segregation of accounts/roles and, where applicable, data segregation policies (e.g., RLS/tenant segregation)

Credential and secret management via dedicated systems/environment variables

16. 3) Application and infrastructure security

Rate limiting, anti-abuse/anti-bot protections, and suspicious pattern detection

- Monitoring, logging, and anomaly detection
- Hardening, patching, and vulnerability management processes according to risk and operational priorities

17. 4) Operational resilience and incident management

Error monitoring and troubleshooting workflows

Incident response and internal escalation processes

Backup and recovery/disaster recovery procedures proportionate to the service configuration

18. 5) Organizational and governance measures

Internal access restrictions on a need-to-know basis

- Review/update of measures according to service evolution, providers, and risks

Coordination with contractual obligations (e.g., DPA, provider security terms), where applicable

D.3 Limitations and breach note

No system is invulnerable. In the event of a personal data breach, the Controller will follow the internal incident handling process and applicable legal obligations, including notifications to authorities/data subjects where required by law.

ATTACHMENT E

DSAR PROCEDURE (GDPR REQUESTS) AND IDENTITY VERIFICATION

E.1 Purpose

This Attachment describes the practical process for handling privacy rights requests (DSAR) where GDPR or other similar laws apply, and the identity verification measures used to prevent unauthorized disclosure, deletion, or modification.

E.2 How to submit a request

Send an email to info@globalmountain.group with subject "GDPR Request - DashaMap" (or equivalent), indicating, where possible:

Account email and/or identifiers useful to identify the account

Type of request (access, rectification, erasure, restriction, portability, objection, consent withdrawal)

Description and context of the request

Any information useful to locate the data involved

E.3 Identity verification (anti-abuse security)

Before executing a request, the Controller may require reasonable identity verification to ensure that the request comes from the data subject or an authorized person.

Verification may take place, depending on the case, through:

Confirmation from the email associated with the account

Request for minimum additional information strictly necessary to verify identity/control of the account

Additional confirmations in case of sensitive requests (e.g., erasure, portability, account takeover risk)

If the Controller cannot identify the requester sufficiently, the request may be suspended or partially denied until adequate verification is provided, within the limits of law.

E.4 Timing and request handling (where GDPR applies)

The Controller responds without undue delay and, in principle, within 1 month of receiving a valid request.

In case of complex or numerous requests, the deadline may be extended within the limits allowed by law; the Controller will provide notice of the extension and the reasons.

If the request cannot be granted in whole or in part, the Controller will provide a reasoned response within the limits required by applicable law.

E.5 Practical effects of erasure requests

In case of valid erasure, the Controller may close the account, delete or de-identify data and contents, revoke active Magic Links/shared resources, except where retention is necessary for legal obligations, fraud prevention, disputes/litigation defense, or temporary backup residues.

E.6 Requests submitted by parents/guardians (minor data)

If the request concerns data of a minor, the Controller may request reasonable proof of parental responsibility/guardianship and the minimum information necessary to identify the account/data to be verified or removed, within the limits of applicable law.

END OF PRIVACY POLICY