COOKIE POLICY - DASHAMAP

Table of Contents

COOKIE POLICY

DASHAMAP

Controlling Version (English)

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

This Cookie Policy describes in a transparent, detailed, and verifiable manner how the DashaMap platform (owned by GLOBAL MOUNTAIN GROUP LLC) uses cookies, technical identifiers, session tokens, local storage technologies, and similar tools (collectively, the “Tracking Tools”) during access to and use of the Service.

This Policy governs, in particular:
• the categories of Tracking Tools used;
• the purposes pursued;
• the logic for collecting and managing preferences and consent;
• relationships with third-party providers and international data transfers;
• the methods by which the User may exercise control, withdrawal, and updating of their choices.

This Cookie Policy is an integral part of the DashaMap legal ecosystem and must be read in conjunction with:
• Terms of Service (ToS)
• Privacy Policy

• AI Transparency & Compliance Notice
• Astrological Disclaimer
• Refund / Billing / Subscription / Credits Policy
• Acceptable Use Policy
• Data Processing Addendum (DPA), where applicable

Use of the Service entails acknowledgement of this Policy.

For optional Tracking Tools, DashaMap applies the consent, refusal, or opt-out mechanisms provided by applicable law based on the jurisdiction, as described in this Policy and in the Preferences Center, Cookie Settings interface, or equivalent consent-management interface where implemented and applicable.

---

1. Controller, Scope, and Governance Principles

The Data Controller for the activities described in this Policy is:
GLOBAL MOUNTAIN GROUP LLC
Contact email: info@globalmountain.group

DashaMap adopts a Privacy by Design & by Default approach, with the objective of:
• limiting the use of Tracking Tools to what is necessary and proportionate;
• proactively blocking optional tools where required by law;
• enabling granular, reversible, and documentable choices;
• maintaining technical evidence suitable to demonstrate compliance (accountability).

This Policy applies, unless otherwise specifically indicated, to DashaMap domains and subdomains under the Company's control, as well as to any web interfaces, PWA, or webviews connected to the Service, to the extent technically and legally applicable. It also covers tracking-related behavior connected to public pages, authentication, pricing and checkout, gifts, one-shot report flows, referral/coupon flows, Certified Astrologers pages, Partner/Dealer pages, AI interactions, PDF/report delivery, and business/white-label interfaces, only where such areas are enabled and under Company control.

---

2. Definitions and Technical Scope

For the purposes of this Policy, "Tracking Tools" means all technologies that enable information to be stored on the User's device or accessed if already stored, as well as technical identifiers used for functional, security, measurement, or personalization purposes.

By way of example and without limitation, this notion includes:
• HTTP cookies (persistent or session)

• Local Storage / Session Storage
• Session and authentication tokens (e.g., JWT or equivalent tokens)
• Anti-fraud and anti-abuse identifiers (e.g., for checkout, security, or anomalous traffic detection)
• Technical identifiers for integrity of the application session
• Pseudonymized technical logs of consent choices
• Client-side or server-side tagging technologies (where used)
• Identifiers associated with embedded content or third-party services (where enabled)

For clarity:
• not every technical identifier has marketing purposes;
• not every tool is subject to prior consent;
• classification depends on the concrete function, the actual configuration, and applicable law.

The operational classification of each single tool (technical name, provider, purpose, duration, category, legal basis, activation status) is maintained in the Technical and Accountability Register (Annexes A–I), subject to periodic review.

---

3. Regulatory Framework and Multi-Jurisdiction Logic

DashaMap may be accessed from multiple jurisdictions. For this reason, the platform adopts a compliance logic that combines:
• prior consent rules (opt-in) where required (e.g., EEA/UK for optional tools subject to ePrivacy/GDPR);
• notice and opt-out / preference signals rules where provided by local laws (e.g., certain US state privacy laws);
• a precautionary approach in case of technical, geographic, or classification uncertainty.

3.1 Precautionary approach principle (Fail-safe)
When the system is not reasonably able to determine reliably the applicable rule prior to the activation of optional tools, DashaMap applies a precautionary configuration that limits activation to strictly necessary tools only until the preference is collected or the applicable rule is correctly determined.

3.2 No implied consent for optional categories (where required)
In jurisdictions requiring prior consent for optional tools, DashaMap does not, as a rule, consider mere use of the site, scrolling, continued browsing, or the User’s

inactivity as valid consent, except as expressly permitted by applicable law and relevant interpretative practice.

3.3 Variation by geographic area, purpose, and technical channel
Preference management methods may vary based on:
• geographic area or applicable rule;
• tool category;
• purpose pursued;
• role of the third-party provider (e.g., processor / independent controller, where applicable);
• technical channel (web app, external checkout, embedded content, PWA, etc.).

Operational details are described in the Dynamic Consent Matrix (Annex C).

---

4. Categories of Tracking Tools

Production alignment note: references to analytics, marketing, referral attribution, embedded content, specific providers, cookies, local storage keys, consent logs, HMAC/equivalent integrity controls, and audit procedures apply only where those tools are actually enabled or implemented in the live DashaMap environment. If a tool or provider is not active, the relevant section is a transparency and governance rule for conditional or future use and does not imply current activation.

DashaMap adopts a functional taxonomy to ensure clarity to the User and internal technical consistency. The effective classification is performed per single tool, and not exclusively by generic labels.

4.1 Category A — Strictly Necessary (Always Active, where exempt from consent)
This category includes technical tools used for purposes essential to providing the Service requested by the User or to the security of the infrastructure, within the limits and exemptions permitted by applicable law.

This category may include, depending on the actual configuration:

1. Security, anti-abuse, and anti-fraud
   o prevention of attacks (e.g., DDoS, malicious bots, API abuse, carding)
   o protection of checkout integrity and transactions
   o detection of anomalous behavior or attempted compromise
2. Authentication and session management
   o login and session maintenance
   o access control to restricted areas
   o technical management of the account and session/authentication tokens

3. Integrity and functional continuity of the Service
   o technical consistency of sessions or application threads
   o continuity of the flow requested by the User
   o prevention of technical errors in delivery of the requested content

4. Storage of privacy/cookie preferences
   o recording and applying choices expressed in the Preferences Center
   o consistent blocking/activation of optional categories
   o technical documentation of withdrawals and preference updates

Important:
• inclusion in Category A depends on the real technical necessity and the actual function of the tool;
• the same provider may use tools belonging to different categories;
• tools originally configured as “necessary” may be reclassified if function, configuration, or purpose changes.

4.2 Category B — Preferences and Personalization (Optional, subject to technical exceptions)
This category includes tools that improve the user experience without being strictly indispensable for providing the basic service, for example:
• storage of UI preferences (theme, layout, language)
• comfort or personalization preferences that are not essential
• settings not necessary for login, security, or technical compliance

If disabled, some preferences may not be remembered and the User may need to reset them at each new session.

4.3 Category C — Analytics / Measurement (Optional, subject to exempt configurations where permitted)
This category includes tools used for:
• aggregated statistical analyses
• measurement of traffic and performance
• understanding of the general use of the platform
• improvement of the product, usability, and operational stability

When such tools are active, DashaMap adopts minimization measures and restrictive configurations compatible with the provider and the applicable regulatory context (e.g., data reduction, anonymization/pseudonymization parameters where available and appropriate).

Any reference to a specific analytics provider does not imply that all its functionalities are active or that all configurations are identical in every jurisdiction.

4.4 Category D — Marketing, Referral, and Attribution (Optional)
This category includes tools used for:
• campaign or referral attribution
• measurement of the effectiveness of external communications/promotions
• management of bonus, invitation, or referral programs
• marketing or remarketing activities, where present

These tools are treated as optional and require the level of consent/opt-out provided by applicable law.

4.5 Category E — Embedded Content / Third Parties with Conditional Loading (if present)
If DashaMap integrates third-party content or components (e.g., videos, maps, widgets, external tools), such elements may set or read their own identifiers.

Where technically feasible and legally required, DashaMap adopts a click-to-load logic or equivalent to prevent loading embedded content before the User's choice or before application of the relevant privacy rule.

---

5. Methods for Collecting Preferences and Managing Consent

5.1 Preferences Center ("Cookie Settings")
DashaMap provides a Preferences Center accessible through the "Cookie Settings" link (or equivalent label) in the footer and/or through another persistent interface.

The Preferences Center allows, depending on applicable law:
• display of categories;
• activation/deactivation of optional categories;
• review of choices already made;
• withdrawal of consent;
• updating of preferences at any time.

Withdrawal or modification of preferences produces effects for the future and is applied as soon as technically possible, as described in Section 7.

5.2 UX transparency principles (Banner / CMP)
DashaMap designs the preference-collection interface with criteria of transparency, proportionality, and intelligibility, with the objective of avoiding misleading, coercive, or unjustifiably unbalanced practices.

In particular, where applicable:
• optional tools remain blocked until a valid User choice;
• refusal or granular management of preferences is made reasonably accessible;
• pre-selected consent for optional categories is not used where not permitted;
• withdrawal is available by means not unjustifiably burdensome compared to acceptance.

Concrete implementations may vary over time for regulatory, technical, or design adaptation, without reducing the User's rights provided by law.

5.3 No undue penalty for refusal of optional categories
Refusal of optional Tracking Tools does not, in and of itself, result in the blocking of essential functions of the Service nor punitive or discriminatory measures against the User.

It is understood that, in the absence of certain optional categories (e.g., preferences/personalization or specific non-essential functionalities), some components of the user experience may be technically less smooth, less personalized, or require manual resets (for example language, theme, interface preferences, or other comfort settings). Such effects constitute technical consequences of the User's choice and of the applied privacy configuration, and not a coercive measure aimed at obtaining consent.

DashaMap designs the Service so as to keep essential functionalities accessible even in the presence of restrictive settings, within the limits of technical feasibility, security, and service architecture.

---

6. Proof of Consent, Accountability, and Technical Registers

6.1 Purpose of the preferences register
For accountability, audit, security, complaint management, and technical reconstruction of events, DashaMap maintains technical evidence relating to the privacy/cookie choices expressed by the User, within the limits of applicable law and in accordance with minimization principles.

6.2 Technical evidence and integrity (pseudonymized logs)
Consent/preference choices may be recorded by means of pseudonymized technical identifiers and integrity mechanisms (e.g., HMAC or equivalent measures), in order to:
• demonstrate that a choice was collected;
• document which version of the UI/policy/CMP configuration was in use;

• record subsequent changes or withdrawals;
• reduce the risk of unauthorized alterations of the registers.

The Company does not treat such registers as absolute and incontestable proof in every circumstance, but as a component of the set of technical compliance evidence, to be interpreted together with other available elements.

6.3 Minimum content of the registers (depending on context)
Technical registers may include, in minimized/pseudonymized form and within the limits of necessity:
• timestamp of the choice;
• version of the Cookie Policy / banner / CMP configuration;
• category(ies) accepted, refused, or not enabled;
• detected global preference signal (e.g., GPC), if present;
• rule/area applied by the compliance engine;
• technical outcome of preference application (block / activation / withdrawal);
• pseudonymous event identifier;
• technical metadata necessary to verify correct operation.

6.4 Separation between consent registers and security registers
Consent/preference registers are conceptually and functionally distinct from security/network registers (e.g., infrastructure logs, anti-fraud, anomaly monitoring), which may be managed with different legal bases, purposes, and retention periods, as described in the Privacy Policy and in internal security documentation.

---

7. Withdrawal, Technical Deletion, and Scrubbing Protocol

7.1 Withdrawal and updating of preferences
The User may modify or withdraw their preferences at any time via the Preferences Center (“Cookie Settings”).

7.2 Technical application of withdrawal
Following withdrawal, DashaMap adopts technically reasonable measures to:
• stop future loading of withdrawn optional tools;
• deactivate tags/scripts categorized as withdrawn;
• request, where necessary, a refresh/reload or a new session initialization to fully apply the new configuration;
• attempt removal of cookies or identifiers managed by the domain/subdomain under the Company’s control, where technically possible.

Some effects of the new privacy configuration may manifest only after refresh/reload, a new session, or re-initialization of the components involved.

7.3 Technical limits of removal
Automatic removal may not immediately or completely eliminate:
• cookies set by third-party domains not directly controlled by the Company;
• identifiers managed by third-party embedded content already loaded prior to withdrawal;
• data already transmitted to a third-party provider prior to withdrawal (which remains subject to the provider's policies for the period prior to withdrawal).

In such cases, DashaMap adopts a future-blocking approach and may provide, where useful, additional guidance on browser tools or third-party settings.

---

8. Browser Preferences, GPC, DNT, and Other Signals

8.1 Browser and device controls
The User may also manage or delete cookies and local data via:
• browser settings;
• device controls;
• privacy extensions or security tools.

Such tools may affect the functioning of the Service (e.g., frequent logouts, session errors, failure to save preferences, or blocking of necessary technical components).

8.2 Global Privacy Control (GPC)
DashaMap undertakes to recognize and treat the Global Privacy Control (GPC) signal as a valid privacy preference to the extent required or permitted by applicable law and compatible with the technical architecture of the Service.

In particular:
• if a GPC signal is detected, DashaMap may apply more restrictive settings for optional categories or activities, in accordance with applicable law;
• the Preferences Center may nevertheless be displayed or made available to ensure transparency, notice, and granular management;
• the handling of GPC may vary by jurisdiction, purpose, and tool category.

8.3 Do Not Track (DNT)
Some browsers transmit "Do Not Track" (DNT) signals. Since there is no uniformly applied technical/legal standard for DNT, DashaMap does not guarantee a uniform response to such a signal.

Where possible, DashaMap favors more modern and verifiable mechanisms (e.g., GPC) and the Preferences Center.

---

9. Third-Party Providers, Roles, and Technical Segregation

DashaMap may engage third-party providers for infrastructure components, authentication, payments, security, analytics, embedded content, or other technical functions.

9.1 Minimization principle and purpose-based access
The Company adopts technically and organizationally reasonable measures to limit providers' access to the data necessary for the specific function provided, including —where relevant and technically applicable—measures such as:
• restrictive script/tag configurations;
• Content Security Policy (CSP);
• segregation of components or iframes;
• conditional loading / click-to-load;
• periodic review of integrations.

Such measures reduce the risk of unnecessary access, but do not constitute an absolute guarantee of the absence of processing by the provider, which remains governed also by the provider's own policies, configurations, and responsibilities.

9.2 Role of providers (processor / independent controller / other)
Depending on the service and purpose:
• some providers may operate as processors;
• others may operate as independent controllers for specific purposes;
• in some cases different roles may coexist for different functions.

Role qualification is indicated, where applicable, in the Provider Register and Role Matrix (Annex B) and/or in the Privacy Policy.

9.3 Contracts, safeguards, and international transfers
Where required by applicable law, DashaMap implements or requires adequate contractual, organizational, and technical measures to govern relationships with providers and international transfers of data.

Such measures may include, depending on the provider, privacy role, jurisdiction, and type of processing:
• a Data Processing Addendum (DPA) or equivalent agreements, where applicable;
• international transfer mechanisms recognized by applicable law (e.g., Standard Contractual Clauses – SCC, adequacy decisions, or other valid instruments at the time

of transfer);
• where relevant, reliance on recognized adequacy or certification frameworks (e.g., EU–US Data Privacy Framework or equivalent instruments), limited to the providers and activities actually covered;
• supplementary technical and organizational measures proportionate to risk (e.g., minimization, segregation, encryption, access controls, restrictive configurations).

The Company evaluates transfers and applicable safeguards contextually and in an updatable manner, taking into account regulatory, supervisory, and case-law developments. The indication of a specific transfer mechanism in this Policy does not imply that it is the only mechanism used for all providers or for all purposes.

---

10. Duration, Storage, and Retention

Tracking Tools may have:
• session duration (deletion upon closing the browser/session);
• persistent duration (until a defined expiration date);
• duration functionally determined by events (e.g., logout, withdrawal, preference reset, token expiration, system reconfiguration).

DashaMap applies retention criteria consistent with:
• the declared purpose;
• technical necessity;
• proportionality;
• legal obligations;
• security and accountability needs.

Technical durations by category and, where possible, by single tool are documented in the Duration, Retention, Withdrawal, and Scrubbing Protocol Matrix (Annex E), subject to periodic updating.

---

11. Cookie Policy Updates and New Consent

The Company may update this Cookie Policy for:
• legislative or regulatory changes;
• technical changes to the platform;
• introduction, removal, or replacement of providers/tools;
• updating of purposes or categories;
• improvements in clarity, transparency, and usability.

11.1 Material changes
In the event of substantial changes affecting the purposes, categories, or processing methods of the Tracking Tools, DashaMap will adopt reasonable information measures and, where required by law, will collect consent again prior to activating the new optional categories/purposes.

11.2 Versioning and traceability
Changes are recorded through internal versioning/changelog systems and/or accountability annexes (Annex G), indicating the update date and the relevant reference version.

---

12. User Obligations and Device-Related Limitations of Liability

The User is required to use the Service lawfully and not to intentionally interfere with the platform's privacy/cookie preference management mechanisms.

In particular, it is prohibited to:

1. fraudulently alter consent flows or the technical mechanisms for applying preferences;
2. deliberately circumvent blocking or gating systems for optional tools in order to compromise the functioning of the Service or compliance registers;
3. unlawfully use automation tools, reverse engineering, or client manipulation to simulate, falsify, or alter preferences, technical events, or consent states.

12.1 User software, extensions, and network configurations
The Company is not responsible for cookies, scripts, headers, identifiers, or other tracking introduced, modified, or made visible by elements outside DashaMap's reasonable control, including by way of example:
• browser extensions;
• antivirus/antimalware software;
• local or network proxies;
• VPNs, DNS filtering, secure browsing gateways;
• automatic translators, toolbars, plugins;
• privacy/security tools installed by the User;
• third-party software or services that intercept, rewrite, inject, or filter web traffic.

Such tools may alter page behavior, add network requests, block resources, inject scripts, or report as "site cookies" elements that are not generated, controlled, or authorized by DashaMap.

It remains understood that the Company, acting in good faith, will take charge of technical reports and, where reasonably possible, will cooperate with the User to distinguish between behavior attributable to the platform and interference due to the User's software or network environment.

---

13. Relationship with the Privacy Policy and Legal Basis

This Cookie Policy specifically governs the use of Tracking Tools.

For broader information on the processing of personal data (categories of data, purposes, legal bases, data subject rights, transfers, general retention periods, privacy contacts), the User must refer to the DashaMap Privacy Policy.

In the event of apparent overlap:
• this Cookie Policy prevails for the specific aspects of classification/management of Tracking Tools;
• the Privacy Policy prevails for the general regulation of personal data processing, unless otherwise expressly indicated.

The Terms of Service and other legal documents remain applicable for contractual profiles, service use, and liability, within the limits permitted by law.

---

14. Contacts, Reports, and Technical Complaints

For reports relating to unexpected cookies, preferences not applied, banner/CMP malfunctions, or requests for clarification regarding this Policy, you may contact:
GLOBAL MOUNTAIN GROUP LLC
Email: info@globalmountain.group
Suggested subject: COOKIE COMPLIANCE – [Account / Email / Brief description]

For faster handling of the request, it is recommended to include:
• approximate date and time of the issue;
• browser and version;
• device / operating system;
• screenshot of the banner or the observed behavior;
• any active privacy extensions (if present);
• any use of VPN / proxy / DNS filtering / secure browser (if present).

ANNEXES SECTION

(INTEGRAL PART)

DASHAMAP COOKIE POLICY

Annexes A–I listed below constitute the technical-operational specification and the accountability basis of this Cookie Policy. They describe, with greater granularity, the classification, control, security, audit, and complaint-management measures applied by DashaMap in relation to the Tracking Tools.

The Annexes are binding as the technical-operational documentation of the Policy and shall be interpreted in a coordinated manner with the main text of the Cookie Policy, the Privacy Policy, and the other applicable legal documents.

In the event of an apparent discrepancy between a general description in the Cookie Policy and a technical detail contained in the Annexes:

1. a coordinated interpretation shall apply that prioritizes the protection of the User's rights and choices;
2. verifiable technical reconstruction of the facts shall be prioritized;
3. the solution most compliant with the applicable law in force and the measures/orders of the competent authority shall apply.

It is understood that no provision of the Annexes may be interpreted as a limitation of, or derogation from, the User's non-derogable rights or the Company's legal obligations.

List of Annexes:
· Annex A — Justified Register and Technical Inventory of Tracking Tools
· Annex B — Third-Party Provider Register, Role Matrix, and Technical/Organizational Measures
· Annex C — Dynamic Consent Matrix (Regions, Categories, Applicable Rules)
· Annex D — Register of Consent Evidence, Log Integrity, and Consistency Audit
· Annex E — Duration, Retention, Withdrawal, and Scrubbing Protocol Matrix
· Annex F — Embedded Content Management, Click-to-Load, and Third-Party Gating
· Annex G — Changelog, Versioning, and Historical Accountability
· Annex H — Support Protocol, Reports, and Technical-Legal Complaint Management
· Annex I — Operational Verification Procedure, Periodic Audits, and Compliance Scanning

---

ANNEX A

JUSTIFIED REGISTER AND TECHNICAL INVENTORY OF TRACKING TOOLS

Integral part of the Cookie Policy — DashaMap

A.1 Purpose, methodology, and classification criteria
This Annex A constitutes the technical-operational inventory of the Tracking Tools used or potentially used by DashaMap in the different areas of the Service (e.g., public site, login, workspace, checkout, embedded content), indicating the functional classification, purpose, and technical-legal justification.

DashaMap does not merely list cookies or identifiers, but documents for each entry:
• actual purpose;
• activation condition (pre-consent, post-consent, user-initiated, login, checkout, etc.);
• applied category;
• duration;
• technical/legal justification of the classification (especially for tools classified as “Necessary”).

Classification is carried out per individual tool, and not per provider as a whole. The same provider may therefore appear in different categories.

Important:
• the persistence technology (e.g., HttpOnly cookies, local storage, session storage, client-side or server-side tokens) may vary depending on the active architecture, framework, deployment method, or production configuration;
• the inventory must reflect the configuration actually detected in periodic scans (Annex I), and not only the theoretical design;
• IDs may not be numerically consecutive for reasons of deprecation, migration, or versioning.

A.2 Minimum data schema of the inventory (audit-ready)
For each entry in Register A, DashaMap maintains—where applicable and reasonably available—the following fields:
• Internal ID
• Name / key / identifier
• Technology (HTTP Cookie, LocalStorage, SessionStorage, token, tag, etc.)
• First-party / Third-party
• Provider / service
• Domain/host that sets or uses the tool
• Path (if cookie)

• Security attributes (Secure / HttpOnly / SameSite), if cookie
• Category (A/B/C/D/E of the Cookie Policy)
• Primary purpose
• Activation condition (e.g., page load, login, checkout, click-to-load, post-consent)
• Logical activation basis (necessary / consent / opt-out / user-initiated)
• Client-side duration (target / max)
• Server-side retention (if relevant)
• Potential international transfers (yes/no + reference to Annex B)
• Technical/legal justification of classification
• Date of last technical verification
• Source of detection (scan, manual test, vendor documentation, CMP inventory, etc.)

A.3 Technical inventory (initial operational version — to be kept updated)
Below is an initial reference table. The actual technical characteristics (in particular domain, attributes, duration, and persistence technology) must be confirmed and updated based on the production configuration.

A-001 — ds_consent_v2 (or equivalent consent/preference identifier, where implemented)
• Technology: HTTP Cookie (first-party) or equivalent CMP identifier
• Provider: DashaMap / CMP or consent-management layer, where implemented
• Category: C-A Necessary (Compliance / Preference Governance)
• Purpose: Store and apply the User's privacy/cookie choice; avoid inconsistent re-presentation of the banner; document the expressed preference
• Activation condition: Upon display/management of the banner or the Preferences Center
• Client-side duration: up to 12 months (unless a different more restrictive configuration applies)
• Technical/legal justification (Shield): Tool necessary to give effect to the User's choice (including refusal) and to support accountability of consent/preference management; without such memory the platform might not apply consistently the choice already expressed
• Notes: Duration must be periodically reassessed in accordance with proportionality and applicable practices/rules

A-002 — __stripe_mid / equivalent Stripe anti-fraud identifier
• Technology: HTTP Cookie or provider anti-fraud identifier (third-party / provider-managed)
• Provider: Stripe (contractual entity applicable based on the account/service)
• Category: C-A Necessary (Payment security / anti-fraud, in checkout context)
• Purpose: Risk scoring, fraud prevention, carding prevention, transaction security
• Activation condition: In checkout context / payment components / payment-related flows
• Client-side duration: according to provider configuration (typically persistent; to be documented precisely in production)
• Technical/legal justification (Shield): Tool technically necessary for the security and

integrity of a service expressly requested by the User (payment), within the limits of the actual configuration
• Notes: Provider role, transfers, and contractual bases are referred to Annex B

A-003 — Authentication access token (e.g., sb-access-token or equivalent)
• Technology: HttpOnly cookie and/or client-side token storage (depends on the active implementation)
• Provider: Supabase / auth infrastructure (or equivalent auth component)
• Category: C-A Necessary (Auth / session)
• Purpose: Maintenance of the authenticated session, access to restricted areas, integrity of the login flow
• Activation condition: Login / account session
• Client-side duration: session or configured short duration (to be inventoried in production)
• Technical/legal justification (Shield): Necessary for authentication and secure management of the User's session
• Notes: The concrete technology (cookies vs client-side storage) must be aligned with the production configuration resulting from Annex I scans and tests

A-004 — Session renewal token (e.g., sb-refresh-token or equivalent)
• Technology: HttpOnly cookie and/or client-side token storage (depends on the active implementation)
• Provider: Supabase / auth infrastructure (or equivalent auth component)
• Category: C-A Necessary (Auth / session continuity)
• Purpose: Controlled session renewal, reduction of requests to re-enter credentials, continuity of use of the restricted area
• Activation condition: Authenticated session
• Client-side duration: configurable (to be documented in production)
• Technical/legal justification (Shield): Necessary for the technical continuity of the authenticated session and the security of the access flow
• Notes: Duration must be consistent with the risk profile and the session management policy

A-005 — _cf_bm (or equivalent bot management identifier, if active)
• Technology: HTTP Cookie / provider security identifier
• Provider: Cloudflare or equivalent security provider, if active
• Category: C-A Necessary (Security / anti-abuse / anti-bot)
• Purpose: Distinguish legitimate traffic from malicious automated traffic; mitigate bot abuse, hostile scraping, DDoS, and other forms of abuse
• Activation condition: Edge protection / infrastructure security
• Client-side duration: short (e.g., minutes), according to provider configuration
• Technical/legal justification (Shield): Security and operational continuity tool for protection of the

service
• Notes: Precise details depend on the provider's active configuration

A-006 — ai_context_id (or equivalent AI contextual session identifier)
• Technology: SessionStorage and/or application session memory
• Provider: DashaMap
• Category: [C-B] Preferences/Functional (non-essential application session continuity) unless reclassified with stated reasons in specific contexts
• Purpose: Maintain contextual consistency of an ongoing AI/interpretative session (thread, flow state, short application memory)
• Activation condition: Use of specific AI interactions requiring continuity of context
• Client-side duration: Session
• Technical/legal justification (Shield): Improves continuity and quality of the experience within the requested flow; its absence may result in loss of context or resets, but it is not necessarily indispensable to all basic functions of the Service
• Notes: If, in a specific implementation, the tool becomes technically indispensable to a function expressly requested, reclassification to C-A must be documented with rationale and tests

A-007 — ui_theme_mode (or equivalent theme preference)
• Technology: LocalStorage / first-party cookie
• Provider: DashaMap
• Category: [C-B] Preferences
• Purpose: Store the User's UI preference (e.g., Light/Dark/Sanctuary mode)
• Activation condition: Explicit User choice / interface personalization
• Client-side duration: Persistent (duration defined by configuration)
• Technical/legal justification (Shield): UI personalization without marketing/profiling purpose
• Notes: Deactivation may require manual UI reset each session

A-008 — lang_pref (or equivalent language preference)
• Technology: first-party cookie and/or LocalStorage
• Provider: DashaMap
• Category: [C-B] Preferences (unless specific technical flows require a security/compliance language)
• Purpose: Store the preferred language of the interface and output content
• Activation condition: User language selection or initial inference followed by confirmation/use
• Client-side duration: up to 6 months (or different configured duration)
• Technical/legal justification (Shield): Improves consistency and usability of the

experience; not intended for marketing or profiling
• Notes: If absent, the Service remains accessible but may require language re-selection

A-009 — Reserved / deprecated ID
• Status: not in use (reserved for versioning/migration)
• Notes: The absence of an active entry with this ID does not imply the use of undeclared trackers

A-010 — _ga / ga* / Google analytics identifiers (if active / where enabled)
• Technology: HTTP Cookie / analytics tagging (post-consent, according to configuration)
• Provider: Google (contractual entity applicable for the service used)
• Category: [C-C] Analytics
• Purpose: Measurement of aggregated statistics, performance, usage flows, and service improvement
• Activation condition: Only according to the applicable consent/opt-out rule and Consent Mode configuration (where used)
• Client-side duration: according to analytics and provider configuration (to be documented in production)
• Technical/legal justification (Shield): Optional measurement for analytics; activation subject to applicable preferences
• Notes: Actual configurations (retention, data sharing settings, Consent Mode, etc.) are documented in Annexes B/C. For GA4, the technical wording must reflect the current service configuration and not legacy models no longer applicable

A-011 — _gcl_au (or equivalent marketing/attribution identifier, if active / where enabled)
• Technology: HTTP Cookie / marketing tagging
• Provider: Google (or other attribution/ads provider, if active)
• Category: [C-D] Marketing / Attribution
• Purpose: Measurement of campaign attribution, referral, and promotional performance (e.g., invitation/referral programs)
• Activation condition: Only upon valid consent or under the applicable opt-out regime
• Client-side duration: according to provider/campaign configuration (e.g., 30–90 days)
• Technical/legal justification (Shield): Optional attribution/marketing tool; not necessary for the essential functions of the Service
• Notes: Details on transfers and roles are referred to Annex B

A.4 Inventory integrity, anti-misclassification, and review process
To reduce the risk of inaccurate classifications:
• each new integration involving storage/access technologies shall be assessed prior to release;
• each reclassification (e.g., from “Necessary” to “Optional” or vice versa) must be justified and recorded in Annex G;
• declared classifications are periodically verified through the tests in Annex I.

A.5 Techniques not used for the Company's own marketing/profiling purposes and limitations
The Company declares that it does not implement, for its own marketing/profiling purposes, covert persistence or tracking techniques (e.g., evercookies, legacy LSOs, invasive fingerprinting for promotional purposes) not declared in this documentation.

It remains understood that:
• certain security/anti-fraud or infrastructure providers may process technical device/network signals for security, fraud prevention, and anti-abuse purposes, within the limits of their respective configurations and policies;
• the Company is not responsible for identifiers or scripts introduced by the User's software, extensions, or network configurations outside DashaMap's reasonable control (see also Section 12.1 of the main Policy and Annex H).

End of Annex A

ANNEX B

THIRD-PARTY PROVIDER REGISTER, ROLE MATRIX, AND TECHNICAL/ORGANIZATIONAL MEASURES

Integral part of the Cookie Policy — DashaMap

B.1 Purpose of the Annex and vendor management principles
This Annex B describes, in technical-operational form:
• the main third-party providers that may be involved in providing the Service;
• the potential privacy role (processor, independent controller, other) for specific functions;
• the minimization, segregation, and control measures adopted by DashaMap;
• the framework of contractual safeguards and applicable international transfers.

The qualification of a provider's role may vary depending on:
• the specific function used;
• the active configuration;
• applicable contractual terms;
• the processing context (e.g., security, payment, analytics, marketing, AI inference).

B.2 Summary provider matrix (operational version)

1. Supabase Inc. (or applicable Supabase group entity) — Database / Auth / Backend Services

• Functions: authentication, session management, database, backend infrastructure (depending on the implemented architecture)
• Privacy role: generally processor for the functions performed on behalf of the Company (subject to specific contractual/technical exceptions)
• Tools/identifiers involved: session/authentication tokens, technical auth and session management identifiers (HttpOnly cookies and/or client-side tokens depending on the active implementation)
• Technical/organizational measures (examples):
o Row Level Security (RLS) or equivalent controls for logical segregation of user data
o secure token/session configurations
o minimized-access policies
o encryption in transit (TLS) and application measures
• Hardening notes:
o the concrete auth persistence technology (cookie vs local storage) must be consistent with Annex A and Annex I tests
o transfer details and contractual safeguards are managed under B.4

2. Stripe (applicable contractual entity) — Payments and anti-fraud
• Functions: checkout, payment management, anti-fraud, risk scoring, tokenization of payment instruments (depending on the integration)
• Privacy role: may operate as processor and/or independent controller for specific purposes related to payments, financial compliance, and anti-fraud, depending on the context and applicable contractual documentation
• Tools/identifiers involved: anti-fraud and payment security identifiers (e.g., __stripe_mid or equivalents), payment UI components
• Technical/organizational measures (examples):
o segregated payment components (e.g., Stripe Elements / isolated iframes, where applicable)
o minimization of data processed directly by DashaMap
o separation of payment flows from marketing/analytics flows
o TLS and access controls
• Hardening notes:
o DashaMap does not process raw card data in cleartext when using tokenization/provider-managed components
o the provider's cookie/identifier operation is limited to the payment and security context, according to the actual configuration

3. Google (e.g., Google Ireland Ltd. and/or Google LLC, depending on the service) — Analytics / Marketing / Tagging (if active)

• Functions: analytics, measurement, marketing/attribution, tag management (only if and when activated)
• Privacy role: may vary by service/purpose/configuration; the qualification must be verified for each product used
• Tools/identifiers involved: analytics/marketing identifiers (e.g., _ga, _gcl_au or equivalents), consent signals (Consent Mode, if implemented)
• Technical/organizational measures (examples):
o pre-consent / post-consent gating under Annex C
o restrictive configurations and minimization (e.g., Consent Mode v2, data sharing settings, parameters available in the service)
o logical separation between analytics and marketing
• Hardening notes:
o in the absence of valid consent (where required), optional tags/cookies remain blocked or operate under restrictive settings compatible with the adopted configuration
o technical documentation must reflect the active service version (e.g., GA4) and not legacy settings no longer applicable

4. AI / LLM supply chain providers (e.g., OpenRouter, OpenAI, other integrated providers) — AI inference (not cookie-specific, but relevant to technical flows)
   • Functions: processing of AI/inference requests via API
   • Privacy role: variable depending on the provider, integration, and applicable terms
   • Tools/identifiers involved: typically not marketing cookies, but server-side or application-side technical session/trace identifiers may be involved
   • Technical/organizational measures (examples):
   o TLS (e.g., TLS 1.2/1.3 or higher versions supported)
   o payload minimization
   o segregation of API keys
   o internal data-sending policies and application controls
   • Hardening notes:
   o DashaMap configures and selects providers/models with settings and contractual conditions compatible, where provided, with restrictions on the use of data for training
   o the effective “provider-by-provider / environment-by-environment” details must be maintained in internal technical documentation and, where relevant, in the Privacy Policy/provider register

B.3 Technical segregation and minimization measures (cross-cutting principles)
DashaMap adopts technically and organizationally reasonable measures to limit

providers' access to data necessary for the specific function, including—where relevant and technically applicable:
• isolated components (iframes or sandboxing, where available in the adopted technology);
• Content Security Policy (CSP) with allowlist/whitelist of permitted domains;
• conditional loading (gating, click-to-load, post-consent);
• separation of analytics/marketing flows from auth/payment/security flows;
• periodic review of integrations and contacted domains;
• access controls and the principle of least privilege on the infrastructure/application side.

Such measures are intended to mitigate the risk of unnecessary processing and unauthorized loading, but do not constitute an absolute guarantee of the absence of any technical risk. Residual limitations are managed through testing, monitoring, and intervention procedures (Annexes H and I).

B.4 Contracts, DPA, international transfers, and applicable frameworks
Where required by applicable law, DashaMap implements or requires adequate contractual, organizational, and technical measures for provider relationships and international data transfers.

Measures may include, depending on the specific case:
• Data Processing Addendum (DPA) or equivalent agreements, where applicable;
• Standard Contractual Clauses (SCC) or other valid transfer instruments;
• applicable adequacy decisions;
• reliance, where relevant, on recognized frameworks (e.g., EU–US Data Privacy Framework), limited to the providers and activities actually covered;
• supplementary technical/organizational measures proportionate to risk.

Indication of a specific mechanism in this Annex does not imply that it is the only mechanism used for all providers or for all purposes.

B.5 Content Security Policy (CSP) and domain control
DashaMap implements a Content Security Policy (CSP) and/or other browser/server-side security controls to limit the loading of scripts, frames, resources, and connections to unauthorized domains.

The CSP:
• substantially reduces the risk of loading unforeseen scripts/trackers;
• supports front-end supply chain control;
• facilitates technical audits (Annex I) and reconstruction of anomalous events (Annex H).

The CSP must be kept consistent with:
• permitted domains and integrations actually active;
• the change log of modifications (Annex G);
• periodic enforcement tests (Annex I).

End of Annex B

ANNEX C

DYNAMIC CONSENT MATRIX

(REGIONS, CATEGORIES, APPLICABLE RULES)

Integral part of the Cookie Policy — DashaMap

C.1 Purpose and operational scope
This Annex C defines the technical-operational enforcement logic of privacy/cookie preferences and relevant signals (e.g., GPC), in relation to:
• geographic area or applicable rule;
• tool category;
• status of the User's choice;
• technical context (public web, login, checkout, embedded content, etc.).

The Matrix describes the expected platform behavior in terms of gating, blocking, selective activation, and signal handling, in compliance with the Cookie Policy and applicable law.

C.2 Enforcement principles (privacy by default and fail-safe)
DashaMap adopts the following principles:

1. Preventive gating of optional tools: where required by law, optional tools are not loaded/initialized prior to the User's valid choice.
2. Restrictive default in case of uncertainty: where it is technically impossible to determine the applicable rule (e.g., uncertain geolocation, signal conflicts), a precautionary configuration is applied that limits activation to necessary tools only.
3. No cookie wall for essential functions: refusal of optional categories does not, in and of itself, block access to the essential functions of the Service, except for specific technical dependencies clearly indicated.
4. No pre-selection (where required): no pre-selection of optional categories where not permitted.

5. Traceability of choices: consent/preference events are recorded in accordance with Annex D.

C.3 Reference categories (aligned with the main Policy and Annex A)
The platform processes signals and applies gating based on the following categories:
• C-A Necessary (Always On): security, auth, anti-fraud, preference governance
• [C-B] Preferences/Functional: UI, language, non-essential functional continuity, personalization
• [C-C] Analytics: measurement and performance
• [C-D] Marketing/Attribution: campaigns, referral, attribution
• [C-E] Embedded/Third-Party Conditional Load: external content subject to click-to-load or specific rules (in coordination with Annex F)

C.4 Baseline geographic matrix (jurisdictional baseline)
The table below represents an operational baseline. Concrete application may vary by type of processing, category, and applicable law.

Area / Applicable rule — C-A Necessary logic — C-B/C-C/C-D logic — Banner/Preferences Center — Browser signals (GPC/DNT) — Operational notes

EEA / EU / EEA
• C-A: Always On (within the limits of applicable exemptions)
• C-B/C-C/C-D: Prior Opt-in (preventive blocking)
• Banner/Preferences Center: Yes, where implemented and required, with preference management and withdrawal
• GPC/DNT: Managed as privacy/preference signals in a manner compatible with law and architecture; they do not necessarily replace all notice interfaces
• Notes: Priority to ePrivacy/GDPR and restrictive default

United Kingdom (UK)
• C-A: Always On
• C-B/C-C/C-D: Prior Opt-in (preventive blocking)
• Banner/Preferences Center: Yes, where implemented and required
• GPC/DNT: Managed compatibly with UK framework and technical implementation
• Notes: Operational alignment with applicable UK rules/practices in force

Switzerland (CH)
• C-A: Always On
• C-B/C-C/C-D: Precautionary configuration oriented to consent/explicit choice for optional tools
• Banner/Preferences Center: Yes, where implemented and required
• GPC/DNT: Supported as privacy/preference signals for hardening of configuration
• Notes: Adaptation based on applicable regulatory framework and regulatory updates

United States (USA)
• C-A: Always On
• C-B/C-C/C-D: Variable rule by purpose and applicable state law; operational baseline oriented to

notice, preferences, and opt-out, with dedicated signal handling (e.g., GPC) where required
• Banner/Preferences Center: Yes, where implemented and required (notice + preference control)
• GPC/DNT: GPC recognized and treated to the extent required/permitted by applicable law; DNT treated as a non-standardized signal (best effort)
• Notes: No assumption of absolute uniformity across States/purposes

Rest of World (ROW) / Uncertain region
• C-A: Always On
• C-B/C-C/C-D: Restrictive precautionary default (opt-in by default until correct determination or choice)
• Banner/Preferences Center: Yes, where implemented and required
• GPC/DNT: Supported according to architecture and availability
• Notes: In case of uncertainty, the more protective configuration prevails

C.5 Consent state matrix (technical behavior)

To avoid ambiguity between security, payment, and analytics/marketing, DashaMap distinguishes flows separately.

User State: Awaiting choice
• C-A Necessary: Active (necessary tools only, compatible with the browsing phase)
• C-B/C-C/C-D: Blocked, where required by the applicable rule
• Edge security/anti-fraud: Active within the limits of technical necessity
• Payment UI (checkout): Activation only if/when the User initiates checkout; payment components segregated according to context
• Analytics/Marketing: Blocked (where opt-in regime or restrictive default applies)
• Consent evidence: Possible log of banner/Preferences Center display

User State: Accepts all optional categories
• C-B/C-C/C-D: Activated according to configuration and categories
• Edge security/anti-fraud: Active
• Payment UI: Active if requested by the User
• Analytics/Marketing: May be activated according to enabled categories
• Consent evidence: Log event “Accept All” + category status + policy/banner version

User State: Refuses optional categories
• Edge security/anti-fraud: Active
• Payment UI: Available if requested by the User and necessary for payment; payment components operate under their own security logic
• Analytics/Marketing: Blocked / denied / not initialized according to configuration
• Consent evidence: Log event “Reject Optional” or equivalent

User State: Granular choice
• C-B/C-C/C-D: Only enabled categories
• Edge security/anti-fraud: Active
• Payment UI: Active if requested by the User

• Analytics/Marketing: Selective loading for consented categories
• Consent evidence: Log mapping of categories ON/OFF

User State: Subsequent withdrawal / preference modification
• C-B/C-C/C-D: Updated according to the new choice (with kill-signal/gating and scrubbing where applicable)
• Edge security/anti-fraud: Active
• Payment UI: Managed according to session/checkout context
• Analytics/Marketing: Future deactivation and scrubbing to the extent technically possible
• Consent evidence: Log event “Revoke/Update” + technical application outcome

C.6 Browser signal management protocol (GPC and DNT)

C.6.1 Global Privacy Control (GPC)
DashaMap recognizes the GPC signal as a valid privacy preference to the extent required or permitted by applicable law and compatibly with the technical architecture of the Service.

In practice:
• detection of GPC may result in a more restrictive configuration for optional categories or activities;
• the Preferences Center may nevertheless be shown or made available to ensure notice, transparency, and granular management;
• the operational meaning of GPC may vary by jurisdiction, purpose, and category (e.g., analytics, marketing, embedded).

C.6.2 Do Not Track (DNT)
The DNT signal, in the absence of a uniformly binding technical/legal standard, is treated as a privacy-hardening signal and best-effort support:
• priority to deactivation/limitation of optional marketing components, where technically compatible;
• no promise of full equivalence to a formally expressed consent regime.

C.7 Geolocation limits and signal conflict management (Geo-IP Fail-safe)
The Company acknowledges that IP-based geolocation is not 100% accurate. To reduce the risk of incorrect application:

1. the system may use multiple indicators (e.g., IP geolocation, browser/language settings, application signals, account data lawfully and proportionately available);

2. in the presence of conflicts or uncertainty, the more restrictive precautionary configuration prevails;
3. the use of account/billing data to determine the privacy rule occurs only if technically necessary, proportionate, and consistent with the declared purposes.

C.8 Alignment with vendor consent management systems (e.g., Google Consent Mode v2, if implemented)
When DashaMap uses Google tools subject to consent, it may implement mechanisms to transmit the consent state (e.g., Consent Mode v2) to align tag behavior with the User's choice.

In the event of refusal of relevant categories or restrictive default:
• tags may remain blocked or receive denial signals according to the adopted configuration;
• the objective is to reduce the collection of client-side identifiers and limit processing to the levels allowed by technical configuration and applicable law;
• the concrete configuration (consent signals, data sharing settings, tag deployment) must be verified in periodic audits.

C.9 Governance, review triggers, and change control
Matrix C is subject to extraordinary review in the event of:
• legislative changes or relevant authority measures/orders;
• material changes to integrations (analytics, marketing, payment, embedded, AI);
• reclassification of tools in Annex A;
• introduction of new privacy signals/browser support;
• incidents or technical complaints requiring review of controls.

Relevant changes must be recorded in Annex G and, where required by law, accompanied by re-consent/notice measures.

End of Annex C

ANNEX D

REGISTER OF CONSENT EVIDENCE, LOG INTEGRITY, AND CONSISTENCY AUDIT

Integral part of the Cookie Policy — DashaMap

D.1 Purpose of the consent evidence register
This Annex D describes the procedure by which DashaMap:
• records privacy-cookie consent/preference events;

• protects the integrity of technical evidence;
• supports audits, complaint management, and reconstruction of events;
• minimizes the use of identifying data in logs.

Consent evidence is not treated as “absolute proof” in the abstract sense, but as a component of an accountability and technical reconstruction system to be assessed together with other elements (application logs, active configuration, changelog, tests, reports).

D.2 Logging integrity (HMAC / equivalent measures)
To protect the integrity of registers and reduce the risk of unauthorized alteration, DashaMap may use:
• pseudonymized event identifiers;
• cryptographic integrity mechanisms (e.g., HMAC-SHA256 or equivalent measures);
• segregation of access to logs;
• key/secret control and periodic rotation, where implemented;
• timestamping and record versioning.

Conceptual (non-prescriptive) example of constructing an event identifier:
• HMAC of the technical context of the event (e.g., combination of timestamp, event metadata, minimized/pseudonymized portions of client context) with an application secret securely managed.

Important:
• pseudonymization does not necessarily equate to anonymization;
• record design must follow the principle of minimization and purpose separation.

D.3 Minimum content of consent/preference records
Each relevant event (e.g., banner display, accept all, reject, granular choice, withdrawal, click-to-load with contextual consent) should include, where applicable:
• timestamp (preferably UTC);
• event type (view / accept / reject / granular_update / revoke / embedded_activation / other);
• Cookie Policy version;
• banner/CMP version or consent UI configuration;
• categories involved and status (ON/OFF/denied/not set);
• rule/area applied by the compliance engine (e.g., baseline opt-in, opt-out, restrictive default);
• presence of relevant browser signals (e.g., GPC detected: yes/no);
• pseudonymous event identifier;
• technical outcome of application (blocked / activated / withdrawal initiated /

scrubbing attempted / other);
• reference to session or technical context (in minimized form) if necessary for troubleshooting.

D.4 Log segregation and access control
DashaMap maintains functional separation between:
• consent/preference logs (privacy-cookie accountability);
• security/network logs (anti-abuse, anti-fraud, technical monitoring);
• application logs (debug, errors, performance), according to internal policies and the Privacy Policy.

Access to logs is restricted to personnel/authorized parties who need them for:
• security,
• compliance,
• audit,
• technical support,
• complaint management.

D.5 Periodic consistency audit protocol (privacy-cookie logging)
The Company performs periodic checks (e.g., every 90 days or with an equivalent frequency defined internally) to verify:

1. Consistency between consent event and observed tag/script behavior.
2. Correct recording of minimum fields.
3. Record integrity (HMAC or equivalent measure).
4. Alignment between policy/banner version and technical configuration in production.
5. Presence of functioning withdrawal/modification paths.

Such checks are coordinated with the technical tests in Annex I.

D.6 Handling of reports and verification requests
In the event of reports concerning unexpected cookies or preferences not applied:
• DashaMap analyzes the available consent/preference record;
• compares the active configuration and the changelog (Annex G);
• verifies any interference due to the User's software or network environment (see Annex H and Section 12.1 of the main Policy).

To enable effective technical verification, the report should include, where possible:
• date/time,
• browser/device,

• screenshot,
• possible HAR/Network log export,
• presence of extensions/VPN/proxy/DNS filtering.

D.7 Evidentiary limits and User rights
Technical consent evidence is an accountability and reconstruction tool; it does not exclude:
• the User's right to submit a complaint or challenge;
• the Company's cooperation obligations;
• the powers of the competent authority to request clarifications, tests, or supplementary documentation.

End of Annex D

ANNEX E

DURATION, RETENTION, WITHDRAWAL, AND SCRUBBING PROTOCOL MATRIX

Integral part of the Cookie Policy — DashaMap

E.1 Purpose and principle of temporal minimization
This Annex E defines:
• target and maximum durations of Tracking Tools (where applicable);
• server-side retention of registers;
• withdrawal and "scrubbing" (active cleaning) logic;
• technical limits of deletion.

DashaMap applies the principle of temporal minimization: a tracking tool should not persist beyond the time necessary for the declared purpose, except for legal obligations, security needs, or adequately justified accountability needs.

E.2 Operational duration matrix (target vs maximum)
The durations indicated below represent an operational baseline. Actual configuration must be verified in production and documented in Annex A.

Category C-A Necessary (Security/Auth)
• Primary purpose: login, auth, security, anti-abuse, anti-fraud
• Target duration: session / configured short duration (e.g., minutes/hours/days, depending on the token/tool)
• Maximum duration: defined by the risk profile and technical configuration
• Hardening logic: short duration and token rotation where possible, to reduce the risk of session compromise

Category C-A Necessary (Compliance / Preference Governance)
• Primary purpose: record/apply the privacy-cookie choice
• Target duration: up to 6–12 months (based on configuration and proportionality assessment)
• Maximum duration: defined by internal policy and applicable regulatory framework
• Hardening logic: duration sufficient for accountability without exceeding the purpose

Category [C-B] Preferences/Functional
• Primary purpose: theme, language, non-essential functional continuity
• Target duration: session up to 6 months (depending on the tool)
• Maximum duration: defined per tool in Annex A
• Hardening logic: limited persistence to balance usability and minimization

Category [C-C] Analytics
• Primary purpose: measurement of use/performance
• Target duration: according to analytics configuration and purpose (e.g., from months to provider-configured durations)
• Maximum duration: to be documented specifically in Annex A
• Hardening logic: activation subject to applicable consent rule; periodic review of retention

Category [C-D] Marketing/Attribution
• Primary purpose: campaign/referral attribution
• Target duration: minimum duration compatible with correct attribution (e.g., 30–90 days, depending on campaign/provider)
• Maximum duration: to be documented specifically in Annex A
• Hardening logic: limited and proportionate duration with respect to the promotional purpose

Category [C-E] Embedded/Third-Party Conditional Load (if present)
• Primary purpose: activation of external content upon request
• Target duration: session or according to provider, if the content is activated
• Maximum duration: dependent on external provider and configuration
• Hardening logic: click-to-load and pre-activation blocking; transparency on transfer to the provider

E.3 Withdrawal and scrubbing protocol (active cleaning)
Within the limits of technical feasibility, DashaMap implements a withdrawal

procedure that does not consist solely in “no longer reading” optional tools, but also includes deactivation and cleaning measures.

Upon withdrawal/modification of preferences:

1. Future gating: loading rules are updated to prevent new initializations of withdrawn categories.
2. Kill-signal/stop logic: optional tags/scripts already controlled by the system are deactivated or not invoked in subsequent interactions.
3. Removal attempt: the system attempts deletion of first-party cookies/identifiers associated with the withdrawn category and under the control of the Company’s domain/subdomain.
4. Outcome tracking: the withdrawal event and technical outcome (scrubbing attempted / completed / partial) may be recorded in Annex D.

E.3.1 Technical limits of scrubbing (carve-out)
Automatic deletion may be partial or deferred in the presence of:
• third-party cookies on domains not directly controlled by the Company;
• embedded content already loaded prior to withdrawal;
• cookies with specific domain/path attributes requiring deletion with identical attributes;
• HttpOnly cookies or other identifiers not directly deletable via JavaScript;
• provider-managed components requiring refresh/reload or a new session to fully reflect the new state.

In such cases, DashaMap:
• prioritizes future blocking of reading/writing and re-triggering of optional scripts;
• applies the new configuration at the first technically useful point (e.g., refresh, new session, new component initialization).

E.4 Server-side log retention (consent and audit)
Consent/preference registers and correlated technical outcomes are retained for a period defined by internal policy, proportionate to the purposes of:
• accountability;
• complaint management;
• audit;
• defense/verification in the event of disputes.

Suggested operational baseline:
• consent/preference logs: up to 12 months, unless specific legal needs or ongoing proceedings;

• periodic audit documentation (test outcomes, screenshots, HAR, reports): up to 3 years or a different period defined internally for compliance needs and proof of diligence.

Actual retention periods must be consistent with the Privacy Policy and internal security/compliance documentation.

End of Annex E

ANNEX F

EMBEDDED CONTENT MANAGEMENT, CLICK-TO-LOAD, AND THIRD-PARTY GATING

Integral part of the Cookie Policy — DashaMap

F.1 Purpose and scope
This Annex F governs the management of third-party embedded content and components (e.g., videos, maps, widgets, chat, external tools) that may involve:
• loading of third-party scripts;
• transfer of technical data (e.g., IP address, user-agent, request metadata);
• setting or reading of identifiers of the external provider.

F.2 Preventive gating principle
Where technically feasible and legally required, DashaMap applies a preventive gating logic:
• embedded content is not automatically loaded on page load;
• an informational placeholder is shown instead;
• loading occurs only after the User's choice (e.g., consent to the relevant category and/or an explicit click-to-load action).

F.3 "Click-to-Load" protocol (activation on the User's initiative)
For content subject to gating, DashaMap adopts—where applicable—the following scheme:

1. Informational placeholder
   In place of the content, a neutral area is displayed with a clear indication that:
   • the content is provided by a third party;
   • activation may involve transfer of technical data to the provider;
   • cookies/identifiers of the external provider may apply.

2. Explicit activation
   The User may choose to activate the content through a voluntary action (e.g., click on “Load content” or equivalent).

3. Scope of activation
   Activation may apply:
   • to the single interaction,
   • to the session,
   • or according to another clearly described configuration,
   without prejudice to coordination with the Preferences Center and the relevant consent category.

4. Minimum traceability
   The activation event may be recorded as a technical preference/embedded activation event (see Annex D), in minimized form and for accountability/troubleshooting purposes.

F.4 Operational limitations and warnings
Click-to-load and gating substantially reduce the risk of undesired transfers prior to activation, but:
• they do not eliminate processing carried out by the provider after content activation;
• they do not replace the external provider’s policies;
• they depend on correct technical configuration of the embedded component and the vendor’s policy.

After activation, processing may also be governed by the external provider’s terms/policies.

F.5 Domain whitelisting and CSP (coordination with Annex B)
For embedded content, DashaMap maintains:
• a whitelist/allowlist of permitted domains;
• a CSP (and/or equivalent controls) consistent with authorized components;
• periodic review procedures to remove domains no longer necessary.

Any domain or connection not authorized by the security configuration should be blocked or reported, within the limits of the actual capability of the active controls.

F.6 Coordination with categories and consent
Embedded content is coordinated with:
• Annex C (Dynamic consent matrix),

• Annex A (inventory of active technologies),
• Annex I (gating verification tests).

In the event of conflict between the category of the embedded content and its technical implementation, the more precautionary approach prevails until the configuration is corrected.

End of Annex F

ANNEX G

CHANGELOG, VERSIONING, AND HISTORICAL ACCOUNTABILITY

Integral part of the Cookie Policy — DashaMap

G.1 Purpose of the changelog
This Annex G records material changes to the Cookie Policy, to integrations impacting the Tracking Tools, to category classifications, and to consent enforcement rules.

The changelog supports:
• historical accountability;
• reconstruction of the active configuration as of a given date;
• internal/external audits;
• complaint management.

G.2 Minimum fields of the change register
For each relevant change, the register should include:
• version (e.g., v1.0, v1.1, v1.2…)
• adoption date
• effective date
• concise description of the change
• nature of the change (technical / legal / banner UX / vendor / classification / security)
• user impact (none / low / medium / high)
• need for re-consent (yes/no/assessment)
• system action taken (e.g., banner update, tag config update, re-scan, communication)
• reference to updated Annexes (A/B/C/D/E/F/I, if applicable)

G.3 Definition of a material change

A “material change” includes, by way of example:

• introduction or removal of a new third-party provider using storage/access technologies;
• introduction of new purposes (e.g., marketing/referral/analytics) or new categories;
• reclassification of a tool among C-A, [C-B], [C-C], [C-D], [C-E];
• changes to international transfer flows;
• substantial changes to the banner/CMP affecting consent collection;
• changes to scrubbing/withdrawal mechanisms;
• modification of the GPC logic or the restrictive default.

G.4 Example change register (initial baseline)

Version: v1.0

• Adoption date: 21/02/2026
• Effective date: 21/02/2026
• Nature of change: Initial publication of the Cookie Policy + Annexes A–I
• User impact: High (introduction of a full governance and accountability framework)
• Re-consent: Initial assessment based on the active configuration and categories already implemented
• System action: Baseline banner/CMP setup, initial inventory, audit procedures

Version: v1.1

• Adoption date: June 21, 2026
• Effective date: June 21, 2026
• Nature of change: Public-policy cleanup and product/technical alignment; updated dates/version; clarified that analytics, marketing, referral attribution, embedded content, consent logs, HMAC/equivalent integrity controls, and audit procedures apply only where active or implemented in production; aligned terminology with the current DashaMap legal framework.
• User impact: Low/Medium (clarity and governance alignment; no activation of optional tools by this document alone)
• Re-consent: Not required by this documentary update alone; re-consent must be assessed separately if optional analytics, marketing, referral attribution, embedded content, or new tracking purposes are activated or materially changed.
• System action: Update Policy/Annexes, verify footer Cookie Settings availability, verify pre-consent blocking for optional tools before publication or activation.

Version: future version

• Adoption date: to be set when adopted
• Effective date: to be set when adopted
• Nature of change: Activation, removal, or material modification of analytics, marketing, referral attribution, embedded content, consent-management tooling, or other tracking technologies.
• User impact: to be assessed at the time of change
• Re-consent: to be assessed under applicable law and the active technical configuration

• System action: update gating, banner/CMP or equivalent interface, Annexes A/B/C/I, and perform pre/post-release verification where applicable.

G.5 Re-consent protocol (coordination)
Where a material change requires new consent under law or internal policy:
• the platform updates the banner/Preferences Center and CMP configuration;
• the relevant categories/purposes remain blocked until a new choice, where required;
• the changelog records the measure adopted;
• re-consent events are logged in accordance with Annex D.

G.6 Distinction between hotfixes and material changes
Not all technical changes are “material”.
By way of example, the following may not be material:
• security patches that do not introduce new tracking/purposes;
• performance optimizations without impact on categories;
• naming/documentation updates without substantive change.

Such changes may nevertheless be noted in internal technical logs or a concise changelog.

End of Annex G

ANNEX H

SUPPORT PROTOCOL, REPORTS, AND TECHNICAL-LEGAL COMPLAINT MANAGEMENT

Integral part of the Cookie Policy — DashaMap

H.1 Purpose and management principles
This Annex H defines the operational workflow for handling:
• reports of unexpected cookies/identifiers;
• preferences not applied or withdrawals not taken into account;
• suspected gating bypass;
• requests for technical clarification regarding the Cookie Policy;
• requests related to proof of preferences (within legal limits and technical feasibility).

Reports are handled in accordance with the principles of:
• good faith;
• traceability;

• risk containment;
• reasonable technical cooperation;
• protection of the User's rights and compliance with legal obligations.

H.2 Contact channel and data useful for verification
Reports are sent to:
• info@globalmountain.group (or the official channel indicated in the Cookie Policy)

For effective verification, where possible it is recommended to include:
• approximate date and time of the issue;
• URL/page involved;
• browser and version;
• operating system/device;
• screenshots of the banner/Preferences Center and the observed behavior;
• HAR export or network evidence (if available);
• any use of privacy extensions, antivirus, VPN, proxy, DNS filtering, or secure browser.

H.3 Triage and priority classification

Priority 1 — Critical / Suspected Compliance Break
Examples:
• "I refused but an analytics/marketing cookie appears to be active"
• "The banner does not block tags before the choice"
• "Withdrawal not applied"
Actions:
• open a technical ticket with timestamp
• verify CMP/gating/CSP configuration
• reproduce in a test environment and/or controlled production environment
• assess immediate mitigation (e.g., tag blocking, rollback, hotfix)

Priority 2 — Compliance / Accountability / Access to technical clarifications
Examples:
• clarifications on GPC/DNT logic
• request to confirm the category of an identifier
• request for clarifications on consent/preference logs within applicable limits
Actions:
• verify registers (Annex D)
• consult inventory (Annex A) and changelog (Annex G)
• provide a coordinated technical-legal informational response, within permitted limits

Priority 3 — Informational / Usability / General support
Examples:
• “How do I reopen Cookie Settings?”
• clarification on differences between categories
• doubts regarding personalization/language and their persistence
Actions:
• standard support
• operational guidance on browser and preferences
• potential update of FAQs/documentation if useful

H.4 Minimum report handling workflow (audit trail)
For each relevant report, DashaMap should track:
• ticket ID or internal reference
• date/time of receipt
• priority category
• issue summary
• evidence received
• checks performed (e.g., network tests, log review, CSP/CMP review)
• outcome (confirmed / not reproduced / due to user environment / partial)
• corrective actions/mitigations adopted
• closure date and internal owner

H.5 Interference due to the user environment (software/network)
During analysis, DashaMap also verifies the possibility that the observed behavior is influenced by:
• browser extensions;
• antivirus/antimalware;
• proxy/VPN/DNS filtering;
• traffic rewriting tools;
• plugins, toolbars, translators;
• device/browser privacy configurations.

If reasonably plausible interferences emerge, the Company:
• documents them in the ticket;
• informs the User clearly;
• provides, where possible, comparative verification instructions (e.g., testing in a clean/incognito profile without extensions).

H.6 No automatic admission of liability clause
A response to a report, the opening of a technical investigation, adoption of a fix or

mitigation do not, in and of themselves, constitute an admission of liability or automatic acknowledgment of a breach.

Such activities represent the fulfillment of maintenance, security, compliance, and diligent service management duties.

Without prejudice to mandatory applicable laws and the User's non-derogable rights.

H.7 Internal escalation and documentary review
In the event of a confirmed issue impacting consent/categories/tracking:
• escalation is initiated to the technical team and the compliance/privacy lead;
• an update of Annexes A/B/C/D/E/I is assessed;
• the change is recorded in Annex G;
• the need for re-consent/notice to the User is assessed under the main Policy and applicable law.

End of Annex H

ANNEX I

OPERATIONAL VERIFICATION PROCEDURE, PERIODIC AUDITS, AND COMPLIANCE SCANNING

Integral part of the Cookie Policy — DashaMap

I.1 Purpose and frequency
This Annex I defines the minimum periodic technical verification protocol aimed at checking consistency between:
• what is declared in the Cookie Policy and Annexes;
• the configuration actually in production;
• the observable front-end behavior (network, tags, scripts, CSP, gating, withdrawal).

Target baseline frequency, where the relevant tooling is implemented:
• full periodic audit: at least every 90 days or an equivalent internally documented frequency;
• extraordinary audit: in the event of material changes (Annex G), critical complaints, or relevant incidents.

I.2 Minimum test scope (pages/contexts)
Each full audit should include at least:
• Home / public landing
• Pricing / marketing pages
• Login / registration (if present)
• Authenticated area / workspace (e.g., AI interactions)

• Checkout / payment page (if active)
• Pages with embedded content (if present)
• Footer / access to the Preferences Center
• Preference withdrawal flow

I.3 Minimum test environment matrix (reproducibility)
To increase test reproducibility, DashaMap documents at least:
• tested environment (production / staging / other)
• date/time of tests (preferably UTC)
• browser and version (at least 2 major browsers)
• mode (normal / incognito / clean profile)
• device or viewport (desktop; optional mobile/tablet if relevant)
• extensions disabled/enabled (explicitly stated)
• presence/absence of VPN/proxy/DNS filtering
• test region or simulation (if applicable)

I.4 Test protocol (operational baseline)

T-001 — Pre-Consent Lockdown (optional tools)
• Objective: verify that, prior to the User's choice (in opt-in regimes or restrictive defaults), optional tools not permitted are not initialized
• Methodology:
o open the page in an incognito window/clean profile
o inspect the Network/Storage tabs
o verify the absence of requests that set/read optional analytics/marketing identifiers prior to the choice
• Expected result:
o no optional cookies/identifiers active prior to consent in contexts where preventive blocking is required
• Evidence to save:
o banner/CMP screenshot
o Storage/Network tab screenshot
o HAR (if available)

T-002 — CSP / Domain Allowlist Enforcement
• Objective: verify that unauthorized resources/scripts are blocked or not loaded
• Methodology:
o attempt to load a script/resource from a domain not in the allowlist (in a controlled environment)
o verify CSP enforcement or equivalent control
• Expected result:

o blocking or refusal of loading according to the security configuration
• Evidence:
o console/network log
o screenshot of error/block
o reference to the CSP version in use

T-003 — Consent State Transition & Scrubbing Integrity
• Objective: verify that acceptance, withdrawal, and modification of preferences produce the expected technical effect
• Methodology:
o accept optional categories
o verify selective activation
o withdraw one or more categories
o verify future stop, gating, and scrubbing attempt
• Expected result:
o preference state update
o future blocking of withdrawn tags
o attempt to remove first-party identifiers where technically possible
o any need for refresh/reload documented
• Evidence:
o Preferences Center screenshots before/after
o Storage tab
o network log
o withdrawal event log (if internally accessible)

T-004 — GPC / DNT Behavior Check (if supported)
• Objective: verify the platform's behavior in the presence of browser privacy signals
• Methodology:
o run tests with GPC enabled/disabled (and, where useful, DNT)
o compare banner/CMP state, categories, and network behavior
• Expected result:
o consistent application of the logic described in Annex C and the main Policy
• Evidence:
o browser settings screenshot
o banner/CMP screenshot
o concise network/storage diff

T-005 — Embedded Click-to-Load Gate (if embedded content is present)
• Objective: verify that gated embedded content does not transfer data prior to activation

• Methodology:
o open the page with the embed
o verify presence of a placeholder
o inspect requests to the embed provider prior to click
o click “Load content” and verify activation
• Expected result:
o no provider loading prior to the action (where gating provides for this)
o controlled loading after activation
• Evidence:
o placeholder screenshot
o pre/post-click network log

T-006 — Checkout Segregation & Payment Context Check (if checkout is active)
• Objective: verify that payment components and their identifiers operate in the intended context, without confusion with analytics/marketing
• Methodology:
o initiate the checkout flow
o verify payment components, contacted domains, iframe/component context
o compare with the status of optional categories
• Expected result:
o payment components active in checkout context
o operational distinction between payment security and optional tracking
• Evidence:
o checkout network log
o payment component screenshot
o notes on classification of observed tools (see Annex A/B)

T-007 — AI Context Isolation Check (if AI functions are active)
• Objective: verify that AI context identifiers do not introduce undeclared optional persistent identifiers
• Methodology:
o start an AI session
o inspect storage/session
o verify consistency with Annex A (e.g., ai_context_id or equivalents)
• Expected result:
o consistency between used identifiers and the declared inventory
o absence of marketing cookies/IDs disguised as AI context
• Evidence:
o Storage/SessionStorage tab
o technical notes and screenshots

I.5 Audit outcome register and evidence retention
For each periodic or extraordinary audit, DashaMap retains an internal report with:
• audit date
• environment
• tester/owner
• tests performed
• outcomes (pass/fail/partial)
• issues detected
• severity
• corrective actions / linked tickets
• remediation date
• re-test (if performed)

Evidence (screenshots, HAR, console extracts, concise reports) is retained for the period defined in Annex E / internal compliance policy, without prejudice to higher legal obligations or needs.

I.6 Escalation upon non-compliance or documentary divergences
If an audit identifies:
• undeclared trackers,
• inconsistent classifications,
• non-functioning gating,
• divergences between Annex A/B/C and actual behavior,
the Company must, without unreasonable delay, activate:

1. technical containment (e.g., tag/script blocking, rollback, hotfix),
2. documentation updates (Annexes and/or main Policy),
3. recording in Annex G,
4. assessment of any need for re-consent/notice.

I.7 Limits of the verification protocol
The periodic audit protocol reduces the risk of incorrect configurations or technical drift, but does not eliminate all residual risk arising from:
• sudden provider updates,
• non-uniform browser behavior,
• user-environment interference,
• temporary deployment errors.

For this reason, the control system is based on the combination of:
• periodic audits,

• changelog,
• incident/complaint monitoring,
• remediation procedures.

End of Annex I

END OF ANNEXES SECTION - DASHAMAP COOKIE POLICY