PRIVACY POLICY
VERSION 1.3
LAST REVISED ON: NOVEMBER 09, 2026

This Policy explains how WunderCorp, Inc. ("WunderCorp", "we", "us", "our") handles personal information in connection with its products and services. It includes merchant and Shopify-specific disclosures for Telemio. Product supplements appear after the main policy; Guardian Browser is not the opening section.

COVERED PRODUCTS, WEBSITES AND SERVICES

The "Covered Services" are the WunderCorp websites, products, desktop and mobile applications, developer tools, SDKs, software, APIs, integrations, hosted environments, accounts, downloads and support services listed below, as well as successors and associated domains operated by WunderCorp. A particular provision applies only where the relevant feature or processing activity is actually offered. Third-party sites accessed through our tools are not Covered Services simply because our tools interact with them.

Company and legacy: wundercorp.co (company site); wundership.com (marketplace); builderstudio.dev (legacy tooling)

Agent & automation: o8r.sh (Operate & Run / Operator); agentvm.sh (AgentVM); loki.computer (LokiAgent); walton.bot (WaltonBot)

Model, infrastructure & knowledge: openmodel.sh (OpenModel); doku.sh (Doku); telemio.sh (Telemio observability)

Business, commerce & discovery: supercharger.sh (Supercharger); argent.sh (ArgentShell); x402mpp.sh (x402 discovery)

Search & browsing: guardianbrowser.sh (Guardian Browser)

1. SCOPE AND ROLES

This Policy applies to people who browse our sites, create accounts, use our software, purchase or subscribe, send support inquiries, or interact with features of a Covered Service. Some tools operate locally, through your own cloud/provider account, or through a third-party integration; in those cases third parties may process data under their terms.

For certain business and merchant services, including merchant-configured Telemio integrations, WunderCorp may process data on a merchant’s behalf as a service provider or processor; the merchant generally determines what is collected from its own customers and is responsible for its notices, lawful basis, and consent. For our own account, billing, website and security activities, WunderCorp may act independently as controller/business. Exact legal roles depend on the service and applicable law.

2. INFORMATION WE COLLECT AND RECEIVE

- Account and organization information: name, email, username, organization, account and authentication identifiers, profile details, permissions, settings, support and communications.
- Usage and device information: IP address, browser or app version, device and operating system, request and referrer URLs, approximate location from IP, timestamps, navigation, events, crash diagnostics, cookies or similar identifiers, and security records.
- Payments and subscriptions: plan, billing and transaction identifiers, purchase status, entitlements and limited payment metadata provided by processors such as Stripe or Apple; payment card details are generally handled by the payment processor.

- User-directed content: marketplace listings, posts, documents, repository or file content, model prompts/responses, agent instructions and task results, workspaces, notes, contacts, messages and other content you submit or deliberately connect.
- Technical telemetry: application traces, logs, metrics, exceptions, performance events, real-user monitoring, release/deployment identifiers, infrastructure signals, model/tool calls, token usage and agent-run details collected from an instrumented system.
- Third-party integration data: information you authorize through Shopify, identity providers, APIs, cloud services, webhooks, MCP connections, mail providers and similar integrations, according to the applicable integration and permissions. Please avoid sending passwords, payment-card details, sensitive personal information, or other data not required for your use case into telemetry, logs, prompts or customer support. Third-party content and outputs may incidentally contain personal information.

3. HOW WE USE INFORMATION

- Provide, operate, authenticate, maintain, troubleshoot and improve Covered Services, including search, browsing, downloads, infrastructure, model and agent features.
- Deliver requested integrations, instrumentation, hosted workspaces, workflows, products, merchant analytics and support.
- Process billing, subscriptions, purchases, account changes, service communications and contract obligations.
- Protect our services, investigate abuse, prevent fraud, enforce terms, secure infrastructure and respond to legal requests.
- Produce aggregate or de-identified performance and adoption insights where lawful and consistent with applicable agreements.
- Send optional promotional communications when permitted, with available unsubscribe choices.

4. PRODUCT-SPECIFIC PROCESSING

Telemio — telemetry, observability and Shopify

Telemio provides OpenTelemetry-based observability for backend services, browser sessions, native applications, infrastructure and agentic runs. When a customer instruments an application or sends events to Telemio, the data transmitted may include telemetry attributes, traces, spans, logs, metrics, URLs, timestamps, session or installation identifiers, device information, IP addresses, customer-supplied properties and the content of error or diagnostic records. The customer controls what it instruments and should avoid sending unnecessary personal or sensitive information.

Where a merchant installs or enables the Telemio Shopify application or web pixel, relevant data may include shop domain and store identifiers, app installation/authentication and permission metadata, configured storefront events (such as page, product, cart or checkout milestones), event timestamps, page or product references, referral and browser information, pseudonymous visitor/session identifiers, and performance or conversion measurements. The precise fields depend on the approved Shopify scopes, web pixel configuration and merchant configuration.

Customer, order, checkout and other Shopify records can be protected customer data even without a person’s name. Names, email addresses, phone numbers and billing or shipping addresses are additional protected fields. Telemio should only request or use such fields when necessary, authorized by the merchant and approved by Shopify where required; an installed app or pixel must not be assumed to receive every protected field. We do not describe use of an unrequested protected field as a standard feature.

For merchant-directed analytics, a Shopify merchant is typically responsible for storefront privacy notices and the lawful basis for tracking. Where applicable, Telemio must respect the merchant’s configuration and customer consent or opt-out choices, including relevant analytics, marketing, preferences and sale-of-data signals. Shopify web pixels can use the

initial customer privacy state and consent-change events. Do not use event APIs to circumvent consent controls. The exact deployed consent behavior requires testing before this draft is published.

Telemio uses merchant-provided data to deliver observability and configured analytics, not for unrelated marketing to that merchant's shoppers. Telemio is not intended to collect passwords, raw payment card numbers, or full checkout form entries. Merchants should not send these fields. See Section 8 for retention and security; actual event retention settings and storage controls must be verified against production.

Operate & Run (O8R), LokiAgent, WaltonBot and AgentVM

Automation and agent tools may process task instructions, browser content, URLs, screenshots or page state, files within an approved workspace, connected service content, execution logs, model prompts and outputs, tool results and approvals needed for a requested task. Some work may be local; other features can use provider-hosted models, managed infrastructure or integrations selected by the user. Users should authorize only appropriate workspaces, connections and actions, and review consequential actions.

Supercharger, Wundership and other products

Supercharger may process contacts, introductions, notes, messages, tasks, sales pipeline and follow-up records submitted through agents, email, APIs, imports or workspaces. Wundership may display profile and listing information you intentionally publish. OpenModel, Doku, ArgentShell, x402 discovery, BuilderStudio and related tools may process models, documentation, request metadata, development data, payment-challenge or transaction metadata and support information as needed for their functions.

5. COOKIES, PIXELS, ANALYTICS AND THIRD-PARTY WEBSITES

We may use essential cookies/session storage for sign-in and service operation and analytics technologies where applicable. The prior policy identifies Umami Analytics for website analytics; products may use additional instrumented or third-party analytics where disclosed in context. Whether a particular pixel or cookie is active depends on the site, settings and applicable law. Users may manage browser settings and applicable consent interfaces. Opening a third-party website from Guardian Browser, O8R or another product can disclose normal connection, cookie and request information to that website, subject to its own practices.

6. DISCLOSURES AND SERVICE PROVIDERS

We share information with vendors and subprocessors as needed for hosting, cloud infrastructure, authentication, telemetry, billing, payments, mail delivery, support, fraud prevention, security and integrations. Providers identified in earlier policies include AWS, Amazon Cognito, Stripe, Apple and Umami Analytics. Identity providers can include Apple, Google or Amazon when selected. Product-specific providers can vary with deployment, location and user-selected model or cloud integrations. We may disclose information when lawfully required, to protect rights and safety, or in a business transaction such as a merger or acquisition. We do not sell or rent personal information for third parties' independent direct marketing.

7. CHOICES, CONSENT AND RIGHTS

Where applicable, you may request access, correction, deletion, portability, restriction or objection; opt out of marketing; manage settings and purchases; and exercise rights relating to targeted advertising, data sales/sharing, or automated decisions with significant effects. Merchant shoppers should ordinarily contact the merchant first about information collected on its store; we will assist merchants with applicable requests. Shopify privacy requests may be transmitted using compliance webhooks. We will verify requests and may retain limited records as legally required.

Privacy and GDPR requests: gdpr@wundercorp.co. Digital Services Act or platform-related notices: dsa@wundercorp.co. General support: hellowundership@gmail.com. Merchant-specific information and procedures may also appear in an in-app disclosure or contractual data processing addendum.

8. RETENTION AND SECURITY

Retention varies by record type, customer contract, product settings and legal requirements. We retain information for as long as reasonably necessary for the stated purposes, including account operation, service delivery, security, support, dispute resolution and regulatory obligations, then delete or de-identify it as appropriate. Our previously disclosed target for raw public download IP logs is up to 90 days unless an exception applies (Appendix B). Telemio event and session retention, Shopify event retention, backup deletion windows and post-uninstall handling require exact production-confirmed schedules before publication.

We use administrative, technical and organizational measures designed to safeguard personal information. Applicable Shopify protected customer data requirements call for encryption in transit and at rest, and additional measures for directly identifying fields, such as encrypted backups, segregated test environments, restricted staff access, access logging and incident response. These are requirements to validate for the actual application and are not a representation that deployment testing has been completed. No system is risk-free.

9. INTERNATIONAL TRANSFERS AND CHILDREN

Data may be handled in locations where WunderCorp and its providers operate. When required for cross-border transfers, we use appropriate legal mechanisms and safeguards for the relevant jurisdiction. Covered Services are not directed to children under 13; the general Terms may impose a higher minimum age for accounts or particular products. We do not knowingly solicit personal information from children under 13 and will address verified cases as required by law.

10. UPDATES AND CONTACT

We may update this Privacy Policy from time to time. Material changes will be announced through our site, the date above, and other notices where required. This document should be read with applicable product terms, contracts, merchant disclosures and the supplements below.

WunderCorp, Inc. | https://wundercorp.co | Privacy: gdpr@wundercorp.co | DSA: dsa@wundercorp.co | Support: hellowundership@gmail.com | Postal: 20020 Ashbrook Commons Plaza 110-117, Ashburn, VA 20147.

APPENDIX A — GUARDIAN BROWSER PRIVACY SUPPLEMENT

This Supplement forms part of the WunderCorp, Inc. Privacy Policy. It explains Guardian Browser-specific data practices for the mobile browser, Guardian Agent Search, Guardian Shield, Reader, Guardian Pro, and related services at guardianbrowser.sh. The general Privacy Policy continues to apply.

1. SCOPE

For purposes of the WunderCorp Privacy Policy, Guardian Browser and https://guardianbrowser.sh are Covered Services. References below to "Guardian" or "Guardian Browser" include the Guardian Browser application, Guardian Agent Search, Guardian Shield, Reader, Guardian Pro, related APIs, and supporting account and search infrastructure.

2. WEB BROWSING AND DEVICE-SIDE DATA

When you visit a website in Guardian Browser, the browser must communicate with that website and related network services to load content. The destination website may receive customary connection and request information such as your IP address, user-agent information, requested URLs, cookies, and other web data according to that site's own practices.

Guardian may store certain browser state and preferences on your device, such as tabs, settings, or interface preferences, where needed to provide the browser experience. Optional Guardian features can cause additional information to be processed as described below.

Guardian Browser is not a VPN and does not claim that all browsing traffic remains on-device or that your IP address is hidden from websites you visit.

3. GUARDIAN AGENT SEARCH

When you submit a search, Guardian may send the search query and search settings to WunderCorp-operated API and search infrastructure. Guardian may use a private SearXNG service and may submit the query, or a corrected or intent-enhanced version of the query, to upstream search providers in order to obtain results.

Search processing may include URLs, page titles, snippets, result categories, publisher or merchant information, image URLs, Open Graph or similar public metadata, and other result metadata. Guardian may retrieve public webpages or metadata server-side to improve previews, identify article images, resolve publisher links, organize specialized search results, or improve relevance.

Search experiences can include web, news, images, videos, shopping, finance, travel, discussions, and other contextual categories. Search result data may be cached or logged as reasonably necessary to operate, secure, debug, and improve the service, subject to the general Privacy Policy.

4. READER AND AI-ASSISTED FEATURES

Reader may inspect the rendered webpage and process article-like text, headings, lists, quotes, metadata, and related page structure so the content can be reformatted for reading. Guardian is designed to use content that is available to the browser and is not intended to retrieve hidden subscriber-only content or bypass access controls.

AI text signals, filtering, summaries, agent assistance, and similar features may process text, URLs, metadata, or other content necessary to provide the requested feature. Depending on the feature, processing may occur on-device or through WunderCorp-operated services and service providers. We aim to limit processing to information reasonably necessary for the feature, security, reliability, and support.

5. ACCOUNTS AND SIGN-IN

If you create or use a Guardian account, we may process account and authentication information such as your email address, name where supplied, account identifiers, authentication-provider identifiers, and security or session information. Guardian uses Amazon Cognito and AWS for account and authentication infrastructure.

Where offered, you may authenticate using Sign in with Apple, Google, or Login with Amazon. Those providers may send us identifiers and profile information according to the permissions you grant. Apple may also send account-status notifications associated with Sign in with Apple so we can respond to events such as authorization revocation or account-related changes.

6. GUARDIAN PRO AND APP STORE PURCHASES

On Apple platforms, Apple processes Guardian Pro subscription payments. WunderCorp does not receive your full payment-card number from Apple. We may receive transaction identifiers, product identifiers, entitlement or subscription status, purchase or renewal information, and related records needed to unlock Pro features, restore purchases, provide support, prevent fraud, and maintain transaction records.

7. GUARDIAN SHIELD, BLOCKING, AND PRIVACY CONTROLS

Guardian Shield may evaluate or block certain webpage requests, trackers, scripts, or other web behaviors according to your settings and Guardian's technical rules. The existence of a privacy or blocking feature does not mean that no information is disclosed to websites or network providers. Normal browsing still requires network communication with websites and may involve third-party content, cookies, scripts, or services that Guardian does not control.

8. THIRD PARTIES

- Websites and services you visit receive information according to their own privacy policies. • Search providers may receive search queries or related request information when Guardian obtains search results

through them. • AWS and Amazon Cognito support Guardian infrastructure and authentication. • Apple supports Sign in with Apple and processes App Store subscriptions on Apple platforms. • Google, Amazon, and other identity providers process information when you choose to use their sign-in services. • Merchants, airlines, hotels, rental providers, ride services, publishers, finance sites, and community services receive

information when you open or interact with their websites or services.

9. YOUR CHOICES

You can choose whether to use optional Guardian search, Reader, AI, account, or Pro features. Where Guardian automatically corrects a search query, the interface may allow you to search the original wording instead. You can manage Apple subscriptions through your Apple account and can use available account settings or support channels to request account deletion or other privacy actions.

10. CONTACT AND ADDITIONAL INFORMATION

Guardian Browser product website: https://guardianbrowser.sh. Guardian Browser is offered by WunderCorp, Inc. Privacy requests and other questions may be submitted using the contact information in the WunderCorp Privacy Policy.

This Supplement should be read together with the general WunderCorp Privacy Policy, including its provisions on information collection, service providers, security, legal disclosures, rights and choices, business transfers, retention, and public download logs.

APPENDIX B — PUBLIC DOWNLOADS AND IP ADDRESS LOGS

This supplement applies when you request or download public installers, release files, documentation, media or other public artifacts from a Covered Service.

Information we may collect

We may log IP address, date and time, product, version, file format, artifact ID, download URL or object path, referrer, browser or user-agent information and similar request metadata. This information may be personal information under applicable law.

Why it is used

Logs help us operate downloads, measure release adoption, troubleshoot delivery, maintain reliability, respond to excessive requests, investigate scraping or abuse, prevent fraud, enforce policies and comply with law. Raw download IP logs are not used for direct marketing.

Legal basis, minimization and retention

Where applicable, processing generally rests on our legitimate interests in secure, reliable downloads, or another lawful basis such as a contract or legal obligation. We aim to separate these logs from account profiles where feasible. Our target retention period for raw public download IP logs is up to 90 days, except where a longer period is reasonably necessary for security, fraud prevention, legal, compliance, support, debugging, backups or disputes. Aggregated or de-identified statistics may be retained longer.

Privacy requests

To help locate a log record, a request may need the approximate date, product, artifact and source IP address. Requests may be sent to gdpr@wundercorp.co.