Keix Security Whitepaper v2.1

Keix — Security Whitepaper (v2.1)

Status: v2.1 — 2026-11-09

Marketing Research Systems S.R.L. · Contact: security@keix.com

---

What changed in v2.1

v2.1 brings the document to the verified state of 2026-11-09. Each item below says what is live in production today and what is not yet.

- Removed the draft status. This version replaces the v2 draft of 2026-09-27.
- Multi-factor authentication: users can enrol an authenticator app (TOTP) or a passkey. A per-workspace “require two-factor authentication” setting and a mandatory second factor for platform administrators have been built and tested on the development environment. In production they are not switched on yet, so MFA is optional for every account today.
- Read-access log: since 2026-11-03, production records who viewed or exported personal data. Entries are kept 12 months and then deleted by an automatic job.
- Ingress access logging is on in production, with request headers dropped.
- Log retention is now set: application logs 15 days, traces 15 days, metrics 30 days.
- Retention policy and erasure design: both were approved on 2026-11-05. The component that will carry out erasure automatically across all systems is in development and is not live in production.
- Availability: since 2026-11-03, the authorization service, the identity provider (ZITADEL) and its login interface each run 2 replicas in production, protected by PodDisruptionBudgets.
- Application-level encryption of stored credentials (OAuth tokens, email and SMTP passwords, API keys, secret integration parameters): the code is in production, but it has not been activated there yet, so these credentials are not yet encrypted at application level in production.
- Data Protection Officer: being appointed. The DPO contact is dpo@keix.com.
- The sub-processor list is published at keix.com/legal/sub-processors. The DPA (Art. 28) template is ready and still under legal review.
- Backup retention is stated per system: PostgreSQL 30 days; volume backups daily, kept 30 days; cluster backups weekly, kept 90 days. No restore test has been performed yet.
- The development branch now requires three passing checks: lint, vulnerability scan, and unit tests of the changed modules.
- Corrected the company name to “Marketing Research Systems S.R.L.”, as it is written on keix.com.
- The verification notes that map each claim to its evidence are kept with the internal source of this document; they are no longer part of the published PDF.

What changed in v2 (since v1)

- Removed the “AES-256 (LUKS) at rest” claim. Volumes are encrypted at the infrastructure-provider level (Hetzner); customer-managed volume encryption is planned, not enabled today.
- Removed the “secrets never in git / never in source code” claim. Application credentials live in Kubernetes Secrets; a small number of legacy credentials still embedded in configuration are being moved and rotated.
- Corrected “every administrative access is tracked.” Platform data changes are recorded as immutable events; cluster-level administrative access logging (Kubernetes API server audit log) is planned.
- Corrected the CI-gate description. Type checking runs in the deployment build, not as a separate blocking CI check. The blocking CI checks are lint, container/filesystem vulnerability scanning, a public-endpoint allowlist audit and a secret-literal scan.
- Corrected the branch-protection claim. Production merges require one reviewer, with a logged exception for a small number of designated organization administrators, who may merge without an additional reviewer.
- Replaced the backup description and the “RTO: 4 business hours” target with the verified backup schedule. No restore drill has ever been performed; the first documented drill is scheduled. No recovery-time figure is published until one has been measured.
- Corrected log retention. Traces are retained 15 days. Application logs currently have no automatic deletion configured; a retention limit is being set.
- Replaced “no customer data leaves the EU” with an accurate data-location statement and a pointer to the sub-processor list and its transfer safeguards.
- Replaced “DPA available” with the correct status: a DPA (Art. 28 GDPR) template is being finalised.
- Corrected the erasure-request SLA from 72 hours to 30 days, and noted that automated propagation of erasure across all systems is still being completed.
- Replaced “TLS 1.3 across all traffic” with an accurate description: TLS terminates at the edge; traffic between services inside the cluster is not encrypted today.
- Removed the reference to Hetzner’s ISO/IEC 27001 certification and every other ISO/SOC-type certification claim.
- Replaced the 7-row sub-processor table with the current, company-wide sub-processor list (25 rows), including the Google Analytics 4 row. **Updated again 2026-10-01:** the site’s consent behaviour described in the original v2 draft (GA4 firing unconditionally, fonts loaded ungated, the booking calendar rendering unconditionally) was accurate as of 2026-09-27 but shipped to production the next day — since 2026-09-28, Consent Mode v2 is live in basic mode (GA4 only fires after “measurement” consent), fonts are self-hosted, and the booking calendar and other embeds are click-to-load.
- Corrected the R2 default-jurisdiction migration exception from “two Archimede-related buckets” to the three buckets the owner’s decision actually keeps out of the EU-jurisdiction migration: the ISCC bucket and the two Archimede buckets.

- Marked the incident-response plan and the AI-provider training opt-out as drafted / to verify, rather than as settled fact.
- Added the “Verification notes” appendix at the end of this document, mapping each corrected claim to its evidence (since v2.1 it is no longer in the published PDF).

---

1. Who we are

Marketing Research Systems S.R.L. (Catania, Italy — VAT IT04616530871) develops **Keix**, a *Data Knowledge for Action* platform for connecting, processing, visualizing and acting on business data, with AI supporting every step. We have been working in market research and data analysis since 2008. The current platform is developed and operated entirely within the European Union.

This document describes the technical and organizational measures we use to protect our customers' data. It is meant to help answer security questionnaires (DDQs), the supplier assessments required by the NIS2 directive (Art. 21, supply chain security), and procurement requests.

2. Summary for the assessor

Area	Keix position
Data residency	Production compute and databases are in the EU (Germany, Finland). Some sub-processors are established outside the EU; see §9 for the full list and the safeguards.
Encryption in transit	TLS at the edge (Cloudflare, then Traefik); our public endpoints negotiate TLS 1.3. Traffic between services inside the Kubernetes cluster is not encrypted today.
Encryption at rest	Storage volumes are encrypted at the infrastructure-provider level (Hetzner). Application-level encryption of stored credentials is in the production code but not yet activated there. Customer-managed volume encryption and encrypted backups are not enabled today.
Identity & access	SSO/OAuth through a self-hosted identity provider (ZITADEL). Optional MFA with an authenticator app (TOTP) or a passkey. A per-workspace MFA requirement is built but not yet switched on in production. RBAC and per-workspace isolation.
Audit trail	Event-sourcing: every change to platform data is recorded as an immutable, timestamped event. A read-access log of who viewed or exported personal data has run in production since 2026-11-03. Logging of administrative access at the cluster level is planned.
Secure development	Pull-request workflow with required checks: lint and vulnerability scanning, plus unit tests of the changed modules on the development branch. A logged exception lets designated administrators merge production changes without an additional reviewer.
Backup	Primary database: continuous WAL archiving and daily base backups, kept 30 days. Volumes: daily backups kept 30 days; cluster: weekly backups kept 90 days; search index: daily snapshots. No restore test has been performed yet.
Availability	The authorization service, the identity provider and its login interface run 2 replicas each, with PodDisruptionBudgets. The primary database runs 3 instances. Services that own event-store subscriptions run as a single replica.
Observability	Centralized telemetry (SigNoz, self-hosted, EU). Logs and traces are kept 15 days, metrics 30 days.
Incident response	A documented incident-response plan exists in draft, pending owner/counsel review. A dedicated reporting channel is live.

Area	Keix position
GDPR	The DPA (Art. 28) template is ready and under legal review. The sub-processor list is published. A DPO is being appointed (dpo@keix.com). A retention policy was approved on 2026-11-05. Erasure requests are handled within 30 days; automated erasure across all systems is in development.

3. Infrastructure and data residency

- **Hosting.** Production workloads run on Kubernetes clusters (RKE2) on Hetzner Cloud infrastructure, in datacenters in Nuremberg, Germany (production, 3 nodes) and Helsinki, Finland (backups and other resources). Both are in the EU/EEA.
- **Edge and CDN.** The frontend is served through Cloudflare (Pages and edge network), with points of presence in the European Union.
- **Data location.** Production compute and databases are in the EU (Germany, Finland). Some sub-processors are established outside the EU and process data under Standard Contractual Clauses or another recognized transfer safeguard; §9 gives the full sub-processor list and the safeguard used for each.
- **Object storage.** Workflow-result artifacts, database backups and search-index snapshots are stored in Cloudflare R2. The buckets are currently in R2's default jurisdiction, which carries no EU-residency guarantee. We plan to move all buckets to the EU jurisdiction, except three that stay under Standard Contractual Clauses plus a transfer-impact assessment: the ISCC bucket and the two Archimede buckets (`archimedepromax`, `keix-pg-archimede-prod`).
- **Separate environments.** Development and production run on separate clusters, with their own credentials and lifecycles.

4. Encryption

- **In transit.** External traffic is encrypted with TLS, which terminates at the edge (Cloudflare, then Traefik inside the cluster). Our public endpoints negotiate TLS 1.3. Traffic between services inside the Kubernetes cluster runs on the cluster's private network and is not encrypted today.
- **At rest: volumes and backups.** Storage volumes holding persistent data are encrypted at the infrastructure-provider level (Hetzner). Off-site backup buckets are encrypted at rest by the object-storage provider. Customer-managed volume encryption (LUKS), and encryption of backups by Keix before they leave the cluster, are not enabled today.
- **At rest: stored credentials.** The platform has application-level encryption for the credentials it stores on behalf of users: OAuth access and refresh tokens, email-account API keys and SMTP passwords, webhook secrets, and secret parameters of datasets and workflows. They are sealed with AES-256-GCM before they are written. This code is in production, but it has **not been activated in production yet**: the production encryption key has not been provisioned and existing records have not been migrated. Until that happens, these credentials are protected in production only by the infrastructure-level encryption above. On the development environment the feature has been active, and existing records migrated, since 2026-10-23.
- **Secrets.** Application credentials are held in Kubernetes Secrets, separated per environment. A small number of legacy credentials still embedded in configuration are being moved into Secrets and rotated (in progress). A quarterly rotation and inventory programme starts once the current rotation is complete.

5. Identity, access and isolation

- **Authentication.** Managed through ZITADEL, a self-hosted OIDC identity provider using the PKCE flow. Users log in with OAuth or with credentials.
- **Multi-factor authentication.** Every user can enrol a second factor: an authenticator app (TOTP) or a passkey. Two further controls have been built: a per-workspace “require two-factor authentication” setting, and a mandatory second factor for platform administrators. Both are checked at in-app sign-in and come with a coverage report for workspace owners. They have been tested on the development environment. **In production they are not switched on yet** (the enforcement setting is unset), so MFA is optional for every account in production today, administrators included.
- **Authorization.** Role-based access control (RBAC) at the module and individual-resource level.
- **Customer isolation.** Every resource belongs to a workspace, and every application query filters by workspace. Users of one workspace cannot reach another customer’s data.
- **Administrative access.** Restricted to authorized personnel, over encrypted channels, with strong authentication. Changes to platform data are recorded as immutable events, and reads and exports of personal data are recorded in the read-access log (§7). Logging of administrative access at the cluster level (Kubernetes API server audit log) is planned.

6. Secure development and change management

- **Mandatory review process.** All changes are proposed as pull requests; the source-control platform rejects direct pushes to the development and production branches. Pull requests to the development branch must pass three checks before merging: lint on the changed files, a vulnerability scan, and the unit tests of the changed modules. Pull requests to the production branch must pass lint and the vulnerability scan and need one reviewer. There is one logged exception: a small number of designated organization administrators may merge production pull requests without an additional reviewer.
- **Vulnerability and security scanning.** Every build runs container-image and filesystem vulnerability scanning (Trivy), lint (Biome), a public-endpoint allowlist audit and a secret-literal scan, all as blocking CI checks. Type checking runs in the deployment build (Cloudflare Pages), not as a separate CI gate.
- **GitOps deployment.** Releases go through an automated pipeline with versioned declarative state. Every deploy is traceable (commit, author, timestamp), and the environment can be rebuilt from the configuration repository.
- **Dependency management.** Dependencies are versioned and go through the same vulnerability scanning as application code.

7. Audit trail and observability

- **Native event-sourcing.** The core of the platform is a message store that records, immutably and in order, every command and every domain event affecting platform data. This gives a complete audit trail of changes to platform data *by design*: what changed, and when, can be reconstructed for the whole history of the data.
- **Read-access log.** Since 2026-11-03, production records who viewed or exported personal data. Views are logged in the people, companies, surveys, email, user and administration areas; exports are logged from people, companies, lists, surveys and quotations. Entries are stored in a dedicated database, kept 12 months, and then deleted by an automatic sweeper.
- **Ingress access log.** The ingress controller (Traefik) writes an access log in JSON format, with request headers dropped.
- **Telemetry.** Distributed traces, application logs and errors are centralized, with full context, in a SigNoz stack that is self-hosted in our EU cluster.
- **Retention.** Application logs are kept 15 days, traces 15 days and metrics 30 days, all within the 30-day ceiling set by our retention policy. The daily platform backup also covers the observability stack, so a backup copy of logs can exist for up to 30 more days (§8).

8. Backup and business continuity

- **Transactional data** (primary database, source of truth): continuous WAL archiving to object storage (Cloudflare R2), with a daily base backup and 30-day retention (PostgreSQL via CloudNativePG). The production database cluster runs 3 instances. §3 gives the object-storage jurisdiction status.
- **Search indexes:** a daily snapshot of the search cluster to object storage (Cloudflare R2). Search indexes can also be rebuilt in full from the domain-event store.
- **Platform volumes and cluster configuration:** daily file-system backups of the platform and observability volumes, kept 30 days, and weekly backups of the cluster, kept 90 days. All go to object storage, alongside the versioned GitOps declarative state.
- **Restore testing.** No restore test has been performed to date. We will not publish a recovery-time or recovery-point target until one has been measured in an actual test.
- **Availability.** Since 2026-11-03, the authorization service, the identity provider (ZITADEL) and its login interface each run 2 replicas in production, with PodDisruptionBudgets so that planned maintenance cannot take both replicas down at once. The ZITADEL and login replicas run on separate nodes; the two authorization replicas prefer separate nodes but may share one. Services that own event-store subscriptions (the message store and a few core services) run as a single replica by design, so a restart of one of them briefly interrupts its function.
- **Declarative architecture.** The whole deployment configuration is versioned, so the application environment can be rebuilt from the GitOps repository and the backups described above.

9. Sub-processors

The table below is the current, company-wide sub-processor list for the Keix platform and marketing site, covering the obligation under Art. 28(2)/(4) GDPR to inform customers of sub-processors. It supersedes the shorter, illustrative table in v1.

Name	Service	Data	Region	Safeguard	DPA filed
Hetzner Online GmbH	Compute, storage, network (all self-hosted software below runs on this)	Everything — all platform data at rest and in process memory	Germany, Finland (EU/EEA)	EU processing, no transfer	N — to obtain/file (owner)
Cloudflare, Inc.	Edge/CDN (Pages), object storage (R2), Web Analytics beacon	Frontend assets, request metadata, workflow artifacts, DB/cluster backups, app pageview counts	Default jurisdiction (not EU-committed); edge is global	DPA + SCC (transfer basis, not yet confirmed accepted)	N — to obtain/confirm (owner)
Postmark (Wildbit/ActiveCampaign)	Transactional email (incl. OTP)	Recipient email address, message content	US	DPA + SCC + TIA (kept under this Phase 0/1 per the owner's decision)	N — to obtain/file (owner)
Resend	Site password-reset mail; newsletter confirmation mail	Recipient email address, message content	US	DPA + SCC (to confirm)	N — to obtain/file (owner)
Stripe	Payments	Payment/billing details, name, email	EU/US	Stripe's standard DPA + SCC	N — to obtain/file (owner)
Google — Gemini API	AI features (document analysis, auto-quotation, voice)	Uploaded documents, inbound emails/attachments, live audio — may contain personal data	US (global endpoint, no EU region configured)	DPA + SCC + TIA; planned: Vertex AI EU region, zero-retention, Phase 1	N — to obtain/file (owner)
Google — Maps Geocoding	Address geocoding	Home/business addresses of people, companies, schools	US (server-side call)	DPA + SCC (to confirm)	N — to obtain/file (owner)

Name	Service	Data	Region	Safeguard	DPA filed
Google — OAuth/Workspace APIs	Customer-connected integrations	Whatever the customer's connected Google account exposes	Customer-dependent	Customer-authorized OAuth; Google's own terms	N/A — customer-connected
Google — Calendar	Site only (booking-demo calendar embed)	Booking form data (calendar embed)	US	Click-to-load since 2026-09-28: the calendar iframe renders only after the visitor clicks to load it, or has already given "experience" consent. No longer unconditional. Google Fonts was removed from the site the same date — fonts are now self-hosted, so there is no longer a separate Fonts sub-processor row.	N — to obtain/file (owner)
Google — Analytics (GA4)	Web analytics on keix.com (measurement ID `G-THKLLJP6D0`)	Usage data, pseudonymous client identifiers, visitor IP	US	Consent Mode v2 live since 2026-09-28, in basic mode: all categories default to denied; GA4 only fires, with IP anonymisation, once the visitor grants "measurement" consent. No longer fires unconditionally. Data Privacy Framework/SCC (to confirm)	N — to obtain/file (owner)

Name	Service	Data	Region	Safeguard	DPA filed
Anthropic	AI features	Prompts/content sent to Claude by AI-assisted features	US (global endpoint, no EU region configured)	DPA + SCC + TIA; planned: Vertex AI EU region, zero-retention, Phase 1	N — to obtain/file (owner)
Meta (WhatsApp Business API, Facebook, Instagram)	Customer-connected messaging integrations	Message content and contact identifiers the customer routes through Meta's APIs	Customer-dependent	Customer-authorized; Meta's own terms	N/A — customer-connected
Telegram	Customer-connected bot messaging	Message content and Telegram identifiers the customer routes through the bot	Customer-dependent	Customer-authorized; Telegram's own terms	N/A — customer-connected
BulkGate	SMS	Recipient phone number, message content	Czech Republic	DPA (EU-EU, no transfer expected)	N — to obtain/file (owner)
Fathom	Call transcripts and AI summaries, customer-connected	Call recordings, transcripts, participant names	US	Customer-authorized OAuth; DPA + SCC (to confirm)	N/A — customer-connected; N for platform-level DPA
Mapbox	Map tiles	Location coordinates rendered in the UI; typically no direct personal-data payload	US	DPA (to confirm)	N — to obtain/file (owner)
Apple / Google Wallet	Wallet passes	Cardholder name, card/pass identifiers	US	Apple's/Google's standard pass-issuer terms	N — to obtain/confirm (owner)
Brave	Web search for the Copilot's "find a dataset" tool	The user's search query text, which may contain personal data the user typed	US	DPA (to confirm)	N — to obtain/file (owner)
Chatwoot	Support chat, self-hosted	Support conversation content, contact identifiers	Hetzner, Germany/Finland (EU/EEA)	Self-hosted, no transfer	N/A — not a third-party processor (see Hetzner note)

Name	Service	Data	Region	Safeguard	DPA filed
Zitadel	Identity/auth, self-hosted	Login identity, session and permission data	Hetzner, Germany/Finland (EU/EEA)	Self-hosted, no transfer	N/A — not a third-party processor (see Hetzner note)
SigNoz	Observability, self-hosted	Traces/logs/metrics, may include request metadata	Hetzner, Germany/Finland (EU/EEA)	Self-hosted, no transfer	N/A — not a third-party processor (see Hetzner note)
Typesense / Postgres / Redis	Search index / relational store / cache, self-hosted	All indexed and cached platform data	Hetzner, Germany/Finland (EU/EEA)	Self-hosted, no transfer	N/A — not a third-party processor (see Hetzner note)
mailinput.com	Email deliverability verification. The call was removed from the platform code on 2026-11-05; it stays active in production until the next platform release, and this row is then removed.	The email address the user is typing, sent live to a third party as they type	Unknown — to verify (owner)	DPA (to confirm)	N — to obtain/file (owner)
Zoom	Archimede product only, customer-connected	Meeting/participant data the customer's Archimede workspace exchanges with Zoom	Customer-dependent	Customer-authorized OAuth	N/A — customer-connected

Name	Service	Data	Region	Safeguard	DPA filed
Customer-connected OAuth integrations	GitHub, LinkedIn, Microsoft, HubSpot, Pipedrive, ClickUp, Fathom, GitLab, Sentry, Stripe, Airtable, PagerDuty, Klaviyo, Salesforce, Bitbucket, Mailchimp, Linear, Shopify	Whatever the customer's connected account exposes; data flows only when the customer connects it	Customer-dependent	Customer-authorized OAuth; each provider's own terms	N/A — customer-connected

Customer-authored dataset integrations (workflow blocks the customer configures to call an external API) may send data to hosts the customer chooses; those hosts are the customer's own processors, not Keix sub-processors.

Data sent to AI providers is limited to the content necessary for the feature requested by the user. A contractual opt-out from the use of that content for model training exists with our current AI providers — to verify (owner) before this claim is published. The up-to-date sub-processor list is published at keix.com/legal/sub-processors and also available on request.

10. Personal data protection (GDPR)

- **Roles.** For data processed on the platform on behalf of customers, Marketing Research Systems S.R.L. acts as **data processor** and the customer is the controller. For commercial contact data, Marketing Research Systems S.R.L. is an independent controller.
- **Data Protection Officer.** We are appointing a Data Protection Officer (Art. 37 GDPR). The DPO can be contacted at dpo@keix.com.
- **DPA.** A Data Processing Agreement (Art. 28 GDPR) template with its annexes is ready and under legal review. We will make it available to customers once that review is complete.
- **Data subject rights.** We support access, rectification, portability and erasure requests. A workspace or account export (a ZIP archive with JSON and CSV files) is part of the product. Erasure requests are handled within 30 days.
- **Erasure.** The design for automated erasure across all systems was approved on 2026-11-05. The component that will carry it out is in development: it runs on the development environment in a mode that performs no deletion, and it is not deployed in production. Until it is live, the propagation of erasure across all systems is not yet automated.
- **Retention.** A retention policy covering each class of personal data was approved on 2026-11-05. Under it, customer workspace content is deleted on request, and no later than 30 days after the contract ends. Automatic deletion is being rolled out one data class at a time. In production today, the read-access log sweeper (12 months) is live. Application-log retention is described in §7. Commercial contact data is kept until consent is withdrawn.
- **Impact assessment.** A data protection impact assessment (DPIA) for the platform is in draft.
- **Minimization.** The platform collects only the data needed for the features the customer activates.

11. Incident management

- **Dedicated channel.** security@keix.com.
- **Formal process.** A documented incident-response plan and breach runbook cover severity classification, containment, eradication, communication to affected customers without undue delay, and a documented post-mortem. The plan is drafted and pending owner/counsel review; an annual tabletop exercise is planned.
- **Regulatory notifications.** In the event of a personal data breach, we support customers with their notification obligations (GDPR Art. 33/34). For customers subject to NIS2, our notification commitments are designed to fit the ACN reporting timelines under Art. 23 (24-hour early warning, 72-hour notification).
- **Responsible disclosure.** Security researchers can report vulnerabilities to security@keix.com. We aim to acknowledge within 48 hours and to give a status update within 7 days. We do not take legal action against good-faith reporters.

12. NIS2 — supporting our customers' supply chain

If your company is an essential or important entity under NIS2 (EU Dir. 2022/2555, transposed in Italy by Legislative Decree 138/2024), Art. 21 requires you to assess the security of your ICT suppliers and bind it by contract. To support you, we provide:

- this whitepaper and direct answers to your security questionnaires;
- a DPA (Art. 28) template, ready and under legal review, and a contractual addendum covering incident notification, minimum security requirements and audit rights, both available once finalised;
- the platform's native audit trail (event-sourcing) and the read-access log, to support your checks;
- a commitment to notify you promptly of any incident affecting your data, consistent with your 24/72-hour reporting obligations.

Document last updated: 2026-11-09 (v2.1). For the latest version, the DPA, or any question: security@keix.com