Keix Security Whitepaper v2.1

Keix — Security Whitepaper (v2.1)

Stato: v2.1 — 2026-11-09

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

---

Cosa è cambiato nella v2.1

La v2.1 porta il documento allo stato verificato al 09/11/2026. Per ogni punto indichiamo cosa è attivo oggi in produzione e cosa non lo è ancora.

- Rimosso lo stato di bozza. Questa versione sostituisce la bozza v2 del 27/09/2026.
- Autenticazione a più fattori: gli utenti possono attivare un'app di autenticazione (TOTP) o una passkey. Sono stati realizzati e testati nell'ambiente di sviluppo l'obbligo di secondo fattore per singolo workspace e l'obbligo per gli amministratori di piattaforma. In produzione non sono ancora attivi: oggi l'MFA è facoltativa per tutti gli account.
- Registro degli accessi in lettura: dal 03/11/2026 la produzione registra chi ha visualizzato o esportato dati personali. Le voci sono conservate 12 mesi e poi cancellate da un job automatico.
- In produzione è attivo il log degli accessi all'ingress, senza gli header delle richieste.
- La retention dei log è ora impostata: log applicativi 15 giorni, tracce 15 giorni, metriche 30 giorni.
- Politica di conservazione e progetto della cancellazione: entrambi approvati il 05/11/2026. Il componente che eseguirà la cancellazione automatica su tutti i sistemi è in sviluppo e non è attivo in produzione.
- Disponibilità: dal 03/11/2026 il servizio di autorizzazione, l'identity provider (ZITADEL) e la sua interfaccia di login girano in produzione con 2 repliche ciascuno, protette da PodDisruptionBudget.
- Cifratura applicativa delle credenziali conservate (token OAuth, password email e SMTP, chiavi API, parametri segreti delle integrazioni): il codice è in produzione ma non vi è ancora stato attivato, quindi in produzione queste credenziali non sono ancora cifrate a livello applicativo.
- Responsabile della protezione dei dati (DPO): in corso di nomina. Contatto: dpo@keix.com.
- L'elenco dei sub-processor è pubblicato su keix.com/legal/sub-processors. Il modello di DPA (art. 28) è pronto ed è ancora in revisione legale.
- La retention dei backup è indicata per sistema: PostgreSQL 30 giorni; backup giornalieri dei volumi, conservati 30 giorni; backup settimanali del cluster, conservati 90 giorni. Non è stato ancora eseguito alcun test di ripristino.
- Il ramo di sviluppo richiede ora tre controlli superati: lint, scansione delle vulnerabilità e test unitari dei moduli modificati.
- Ragione sociale corretta in "Marketing Research Systems S.R.L.", come riportata su keix.com.
- Le note di verifica che collegano ogni affermazione alla relativa evidenza restano nella fonte interna di questo documento e non fanno più parte del PDF pubblicato.

Cosa è cambiato nella v2 (rispetto alla v1)

- Rimossa l'affermazione "AES-256 (LUKS) a riposo". I volumi sono cifrati a livello di infrastruttura del provider (Hetzner); la cifratura dei volumi gestita dal cliente è pianificata, non attiva oggi.
- Rimossa l'affermazione "i segreti non sono mai nel repository / nel codice sorgente". Le credenziali applicative risiedono nei Secret di Kubernetes; un numero limitato di credenziali legacy, ancora presenti nella configurazione, è in fase di spostamento e rotazione.
- Corretta l'affermazione "ogni accesso amministrativo è tracciato". Le modifiche ai dati di piattaforma sono registrate come eventi immutabili; la registrazione degli accessi amministrativi a livello di cluster (audit log del Kubernetes API server) è pianificata.
- Corretta la descrizione dei controlli CI bloccanti. Il type-checking viene eseguito nella build di deploy, non come controllo CI bloccante separato. I controlli CI bloccanti effettivi sono: lint, scansione delle vulnerabilità di container e filesystem, verifica dell'allowlist degli endpoint pubblici e scansione dei segreti letterali nel codice.
- Corretta l'affermazione sulla branch protection. I merge sul ramo di produzione richiedono un revisore, con un'eccezione tracciata per un numero limitato di amministratori dell'organizzazione designati, che possono effettuare il merge senza un revisore aggiuntivo.
- Sostituita la descrizione dei backup e l'obiettivo "RTO: 4 ore lavorative" con la pianificazione verificata. Nessun test di ripristino è mai stato eseguito; il primo test documentato è pianificato. Non viene pubblicato alcun tempo di ripristino finché non sarà misurato.
- Corretta la retention dei log. Le tracce sono conservate 15 giorni. I log applicativi non hanno oggi alcuna cancellazione automatica configurata; è in fase di definizione un limite di retention.
- Sostituita l'affermazione "nessun dato cliente lascia l'Unione Europea" con una dichiarazione accurata sulla localizzazione dei dati e un rimando all'elenco dei sub-processor e alle relative garanzie di trasferimento.
- Sostituita l'affermazione "DPA disponibile" con lo stato corretto: un modello di DPA (art. 28) è in fase di finalizzazione.
- Corretto l'SLA per le richieste di cancellazione, da 72 ore a 30 giorni, precisando che la propagazione automatica della cancellazione su tutti i sistemi è ancora in fase di completamento.
- Sostituita l'affermazione "TLS 1.3 su tutto il traffico" con una descrizione accurata: il TLS termina all'edge; il traffico tra servizi all'interno del cluster non è oggi cifrato.
- Rimosso il riferimento alla certificazione ISO/IEC 27001 di Hetzner e ogni altra affermazione di certificazione di tipo ISO/SOC.
- Sostituita la tabella dei sub-processor (7 righe) con l'elenco completo e aggiornato, a livello aziendale (25 righe), inclusa la riga Google Analytics 4. **Aggiornato nuovamente il 01/10/2026:** il comportamento del sito rispetto al consenso descritto nella bozza v2 originale (GA4 attivo senza condizioni, font caricati senza gate, calendario di prenotazione renderizzato senza condizioni) era accurato al 27/09/2026 ma la correzione è stata distribuita in produzione il giorno successivo — dal 28/09/2026 il Consent Mode v2 è attivo in modalità base (GA4 si attiva solo dopo il consenso "measurement"), i font sono self-hosted e il calendario di prenotazione e gli altri embed sono click-to-load.
- Corretta l'eccezione alla migrazione della giurisdizione predefinita di R2, da "due bucket collegati ad Archimede" ai tre bucket effettivamente esclusi dalla migrazione secondo la decisione del titolare: il bucket ISCC e i due bucket Archimede.
- Segnalati come bozza/da verificare il piano di gestione incidenti e la clausola di opt-out dall'addestramento dei modelli AI, invece di presentarli come fatti consolidati.
- Aggiunta in fondo al documento l'appendice "Note di verifica", che collega ogni affermazione corretta alla relativa evidenza (dalla v2.1 non è più nel PDF pubblicato).

1. Chi siamo

Marketing Research Systems S.R.L. (Catania, Italia — P.IVA 04616530871) sviluppa **Keix**, una piattaforma di *Data Knowledge for Action*: connessione, elaborazione, visualizzazione e attivazione dei dati aziendali, con l'AI a supporto di ogni passaggio. Operiamo dal 2008 nel settore della ricerca di mercato e dell'analisi dati; la piattaforma attuale è interamente sviluppata e gestita nell'Unione Europea.

Questo documento descrive le misure tecniche e organizzative con cui proteggiamo i dati dei nostri clienti. Serve a rispondere ai questionari di sicurezza (DDQ), alle valutazioni dei fornitori richieste dalla direttiva NIS2 (art. 21, sicurezza della supply chain) e alle richieste degli uffici acquisti.

2. Sintesi per il valutatore

Area	Posizione di Keix
Residenza dei dati	Compute e database di produzione sono nell'UE (Germania, Finlandia). Alcuni sub-processor sono stabiliti fuori dall'UE: elenco completo e garanzie al § 9.
Cifratura in transito	TLS all'edge (Cloudflare, poi Traefik); i nostri endpoint pubblici negoziano TLS 1.3. Il traffico tra servizi all'interno del cluster Kubernetes oggi non è cifrato.
Cifratura a riposo	I volumi di storage sono cifrati a livello di infrastruttura del provider (Hetzner). La cifratura applicativa delle credenziali conservate è nel codice di produzione ma non vi è ancora attiva. La cifratura dei volumi gestita da Keix e i backup cifrati oggi non sono attivi.
Identità e accessi	SSO/OAuth tramite un identity provider self-hosted (ZITADEL). MFA facoltativa con app di autenticazione (TOTP) o passkey. L'obbligo di MFA per workspace è realizzato ma non ancora attivo in produzione. RBAC e isolamento per workspace.
Audit trail	Event-sourcing: ogni modifica ai dati di piattaforma è registrata come evento immutabile con timestamp. Dal 03/11/2026 è attivo in produzione un registro di chi ha visualizzato o esportato dati personali. La registrazione degli accessi amministrativi a livello di cluster è pianificata.
Sviluppo sicuro	Flusso a pull request con controlli obbligatori: lint e scansione delle vulnerabilità, più i test unitari dei moduli modificati sul ramo di sviluppo. Un'eccezione tracciata consente ad amministratori designati di effettuare il merge in produzione senza un revisore aggiuntivo.
Backup	Database principale: archiviazione WAL continua e base backup giornaliero, conservati 30 giorni. Volumi: backup giornalieri conservati 30 giorni; cluster: backup settimanali conservati 90 giorni; indice di ricerca: snapshot giornalieri. Nessun test di ripristino è stato ancora eseguito.
Disponibilità	Servizio di autorizzazione, identity provider e interfaccia di login girano con 2 repliche ciascuno, con PodDisruptionBudget. Il database principale gira con 3 istanze. I servizi che gestiscono le sottoscrizioni all'event store girano con una sola replica.
Osservabilità	Telemetria centralizzata (SigNoz, self-hosted, UE). Log e tracce conservati 15 giorni, metriche 30 giorni.
Gestione incidenti	Esiste un piano documentato di gestione degli incidenti, in bozza, in attesa di revisione del titolare/legale. È attivo un canale dedicato per le segnalazioni.
GDPR	Il modello di DPA (art. 28) è pronto ed è in revisione legale. L'elenco dei sub-processor è pubblicato. È in corso la nomina del DPO (dpo@keix.com). Una politica di conservazione è stata approvata il 05/11/2026. Le richieste di cancellazione sono evase entro 30 giorni; la cancellazione automatica su tutti i sistemi è in sviluppo.

3. Infrastruttura e residenza dei dati

- **Hosting.** I carichi di produzione girano su cluster Kubernetes (RKE2) su infrastruttura Hetzner Cloud, in datacenter a Norimberga, Germania (produzione, 3 nodi) e a Helsinki, Finlandia (backup e altre risorse), entrambi nell'UE/SEE.
- **Edge e CDN.** Il frontend è servito tramite Cloudflare (Pages e rete edge), con punti di presenza nell'Unione Europea.
- **Localizzazione dei dati.** Compute e database di produzione sono nell'UE (Germania, Finlandia). Alcuni sub-processor sono stabiliti fuori dall'UE e trattano i dati sulla base di Clausole Contrattuali Standard o di un'altra garanzia di trasferimento riconosciuta; il § 9 riporta l'elenco completo dei sub-processor e la garanzia adottata per ciascuno.
- **Object storage.** Gli artefatti dei risultati dei workflow, i backup dei database e gli snapshot dell'indice di ricerca sono conservati su Cloudflare R2. I bucket sono oggi nella giurisdizione predefinita di R2, che non garantisce la residenza nell'UE. È pianificato lo spostamento di tutti i bucket nella giurisdizione UE, tranne tre che restano sotto Clausole Contrattuali Standard con valutazione d'impatto del trasferimento: il bucket ISCC e i due bucket Archimede (`archimedepromax`, `keix-pg-archimede-prod`).
- **Ambienti separati.** Sviluppo e produzione girano su cluster distinti, con credenziali e cicli di vita indipendenti.

4. Cifratura

- **In transito.** Il traffico esterno è cifrato con TLS, che termina all'edge (Cloudflare, poi Traefik all'interno del cluster). I nostri endpoint pubblici negoziano TLS 1.3. Il traffico tra servizi all'interno del cluster Kubernetes viaggia sulla rete privata del cluster e oggi non è cifrato.
- **A riposo: volumi e backup.** I volumi di storage che ospitano dati persistenti sono cifrati a livello di infrastruttura del provider (Hetzner). I bucket dei backup off-site sono cifrati a riposo dal provider di object storage. La cifratura dei volumi gestita da Keix (LUKS) e la cifratura dei backup da parte di Keix prima che lascino il cluster oggi non sono attive.
- **A riposo: credenziali conservate.** La piattaforma dispone di una cifratura applicativa per le credenziali che conserva per conto degli utenti: token OAuth di accesso e di refresh, chiavi API e password SMTP degli account email, segreti dei webhook, parametri segreti di dataset e workflow. Vengono cifrate con AES-256-GCM prima di essere scritte. Il codice è in produzione, ma **in produzione non è ancora stato attivato**: la chiave di cifratura di produzione non è stata ancora predisposta e i record esistenti non sono stati migrati. Fino ad allora, in produzione queste credenziali sono protette solo dalla cifratura a livello di infrastruttura descritta sopra. Nell'ambiente di sviluppo la funzione è attiva, con i record esistenti migrati, dal 23/10/2026.
- **Segreti.** Le credenziali applicative sono conservate nei Secret di Kubernetes, separati per ambiente. Un numero limitato di credenziali legacy ancora presenti nella configurazione è in fase di spostamento nei Secret e di rotazione (in corso). Un programma trimestrale di rotazione e inventario partirà al termine della rotazione in corso.

5. Identità, accessi e isolamento

- **Autenticazione.** Gestita tramite ZITADEL, un identity provider OIDC self-hosted che usa il flusso PKCE. Gli utenti accedono con OAuth o con credenziali.
- **Autenticazione a più fattori.** Ogni utente può attivare un secondo fattore: un'app di autenticazione (TOTP) o una passkey. Sono stati realizzati altri due controlli: l'impostazione "richiedi l'autenticazione a due fattori" per singolo workspace e l'obbligo di secondo fattore per gli amministratori di piattaforma. Entrambi sono verificati all'accesso in app e includono un report di copertura per i proprietari del workspace. Sono stati testati nell'ambiente di sviluppo. **In produzione non sono ancora attivi** (l'impostazione di enforcement non è valorizzata): oggi in produzione l'MFA è facoltativa per tutti gli account, amministratori compresi.
- **Autorizzazione.** Controllo degli accessi basato sui ruoli (RBAC) a livello di modulo e di singola risorsa.
- **Isolamento tra clienti.** Ogni risorsa appartiene a un workspace e ogni query applicativa filtra per workspace. Gli utenti di un workspace non possono raggiungere i dati di un altro cliente.
- **Accessi amministrativi.** Limitati al personale autorizzato, su canali cifrati e con autenticazione forte. Le modifiche ai dati di piattaforma sono registrate come eventi immutabili, e le letture e le esportazioni di dati personali sono registrate nel registro degli accessi in lettura (§ 7). La registrazione degli accessi amministrativi a livello di cluster (audit log del Kubernetes API server) è pianificata.

6. Sviluppo sicuro e gestione delle modifiche

- **Processo di revisione obbligatorio.** Tutte le modifiche sono proposte come pull request; la piattaforma di controllo versione rifiuta i push diretti sui rami di sviluppo e di produzione. Le pull request verso il ramo di sviluppo devono superare tre controlli prima del merge: lint sui file modificati, scansione delle vulnerabilità e test unitari dei moduli modificati. Le pull request verso il ramo di produzione devono superare lint e scansione delle vulnerabilità e richiedono un revisore. È prevista un'eccezione tracciata: un numero limitato di amministratori designati dell'organizzazione può effettuare il merge delle pull request di produzione senza un revisore aggiuntivo.
- **Scansione delle vulnerabilità e controlli di sicurezza.** Ogni build esegue la scansione delle vulnerabilità di immagini container e filesystem (Trivy), il lint (Biome), la verifica dell'allowlist degli endpoint pubblici e la scansione dei segreti letterali, tutti come controlli CI bloccanti. Il type-checking viene eseguito nella build di deploy (Cloudflare Pages), non come controllo CI separato.
- **Deploy GitOps.** I rilasci passano da una pipeline automatica con stato dichiarativo versionato. Ogni deploy è tracciabile (commit, autore, timestamp) e l'ambiente può essere ricostruito dal repository di configurazione.
- **Gestione delle dipendenze.** Le dipendenze sono versionate e passano dalla stessa scansione delle vulnerabilità del codice applicativo.

7. Audit trail e osservabilità

- **Event-sourcing nativo.** Il cuore della piattaforma è un message store che registra, in modo immutabile e ordinato, ogni comando e ogni evento di dominio che riguarda i dati di piattaforma. Ne deriva *by design* un audit trail completo delle modifiche ai dati di piattaforma: cosa è cambiato, e quando, è ricostruibile per l'intera storia dei dati.
- **Registro degli accessi in lettura.** Dal 03/11/2026 la produzione registra chi ha visualizzato o esportato dati personali. Le visualizzazioni sono registrate nelle aree persone, aziende, sondaggi, email, utenti e amministrazione; le esportazioni da persone, aziende, liste, sondaggi e preventivi. Le voci sono conservate in un database dedicato per 12 mesi e poi cancellate da un processo automatico.
- **Log degli accessi all'ingress.** L'ingress controller (Traefik) scrive un log degli accessi in formato JSON, senza gli header delle richieste.
- **Telemetria.** Tracce distribuite, log applicativi ed errori sono centralizzati, con il contesto completo, in uno stack SigNoz self-hosted nel nostro cluster UE.
- **Retention.** I log applicativi sono conservati 15 giorni, le tracce 15 giorni e le metriche 30 giorni, tutti entro il limite di 30 giorni fissato dalla nostra politica di conservazione. Il backup giornaliero della piattaforma include anche lo stack di osservabilità, quindi una copia di backup dei log può esistere per altri 30 giorni al massimo (§ 8).

8. Backup e continuità operativa

- **Dati transazionali** (database principale, fonte di verità): archiviazione WAL continua su object storage (Cloudflare R2), con base backup giornaliero e retention di 30 giorni (PostgreSQL tramite CloudNativePG). Il cluster di database di produzione gira con 3 istanze. Lo stato della giurisdizione dell'object storage è al § 3.
- **Indici di ricerca:** uno snapshot giornaliero del cluster di ricerca su object storage (Cloudflare R2). Gli indici di ricerca possono anche essere ricostruiti per intero dall'event store di dominio.
- **Volumi di piattaforma e configurazione del cluster:** backup giornalieri a livello di file system dei volumi della piattaforma e dell'osservabilità, conservati 30 giorni, e backup settimanali del cluster, conservati 90 giorni. Vanno tutti su object storage, accanto allo stato dichiarativo GitOps versionato.
- **Test di ripristino.** Ad oggi non è stato eseguito alcun test di ripristino. Non pubblicheremo obiettivi di tempo o di punto di ripristino finché non saranno stati misurati con un test reale.
- **Disponibilità.** Dal 03/11/2026 il servizio di autorizzazione, l'identity provider (ZITADEL) e la sua interfaccia di login girano in produzione con 2 repliche ciascuno, con PodDisruptionBudget, così che la manutenzione pianificata non possa fermare entrambe le repliche insieme. Le repliche di ZITADEL e del login girano su nodi diversi; le due repliche del servizio di autorizzazione preferiscono nodi diversi ma possono condividerne uno. I servizi che gestiscono le sottoscrizioni all'event store (il message store e alcuni servizi core) girano per scelta con una sola replica, quindi il riavvio di uno di essi ne interrompe brevemente la funzione.
- **Architettura dichiarativa.** L'intera configurazione di deploy è versionata: l'ambiente applicativo può essere ricostruito dal repository GitOps e dai backup descritti sopra.

9. Sub-processor

La tabella seguente è l'elenco completo e aggiornato, a livello aziendale, dei sub-processor della piattaforma Keix e del sito di marketing, e copre l'obbligo, previsto dall'art. 28(2)/(4) GDPR, di informare i clienti dei sub-processor. Sostituisce la tabella più breve e illustrativa presente nella v1.

Nome	Servizio	Dati	Regione	Garanzia	DPA depositato
Hetzner Online GmbH	Compute, storage, rete (tutto il software self-hosted sotto elencato gira qui)	Tutto — tutti i dati di piattaforma a riposo e in memoria di processo	Germania, Finlandia (UE/SEE)	Trattamento UE, nessun trasferimento	N — da ottenere/depositare (titolare)
Cloudflare, Inc.	Edge/CDN (Pages), object storage (R2), beacon Web Analytics	Asset frontend, metadati di richiesta, artefatti dei workflow, backup DB/cluster, conteggi pageview app	Giurisdizione predefinita (non impegnata UE); l'edge è globale	DPA + SCC (base di trasferimento, accettazione non ancora confermata)	N — da ottenere/confermare (titolare)
Postmark (Wildbit/ActiveCampaign)	Email transazionali (incl. OTP)	Indirizzo email del destinatario, contenuto del messaggio	USA	DPA + SCC + TIA (mantenuto in questa Fase 0/1 per decisione del titolare)	N — da ottenere/depositare (titolare)
Resend	Email di reset password del sito; email di conferma newsletter	Indirizzo email del destinatario, contenuto del messaggio	USA	DPA + SCC (da confermare)	N — da ottenere/depositare (titolare)
Stripe	Pagamenti	Dati di pagamento/fatturazione, nome, email	UE/USA	DPA standard Stripe + SCC	N — da ottenere/depositare (titolare)
Google — Gemini API	Funzionalità AI (analisi documenti, auto-quotazione, voce)	Documenti caricati, email/allegati in ingresso, audio live — può contenere dati personali	USA (endpoint globale, nessuna regione UE configurata)	DPA + SCC + TIA; pianificato: regione UE su Vertex AI, zero-retention, Fase 1	N — da ottenere/depositare (titolare)
Google — Maps Geocoding	Geocodifica indirizzi	Indirizzi di residenza/attività di persone, aziende, scuole	USA (chiamata server-side)	DPA + SCC (da confermare)	N — da ottenere/depositare (titolare)
Google — API OAuth/Workspace	Integrazioni collegate dal cliente	Ciò che l'account Google collegato dal cliente espone	Dipende dal cliente	OAuth autorizzato dal cliente; termini propri di Google	N/A — collegato dal cliente

Nome	Servizio	Dati	Regione	Garanzia	DPA depositato
Google — Calendar	Solo sito (embed calendario demo)	Dati del form di prenotazione (embed calendario)	USA	Click-to-load dal 28/09/2026: l'iframe del calendario si carica solo dopo che il visitatore clicca per caricarlo, o ha già dato il consenso "experience". Non più incondizionato. Google Fonts è stato rimosso dal sito nella stessa data — i font sono ora self-hosted, quindi non esiste più una riga Fonts separata.	N — da ottenere/depositare (titolare)
Google — Analytics (GA4)	Web analytics su keix.com (ID di misurazione `G-THKLLJP6D0`)	Dati di utilizzo, identificativi client pseudonimi, IP del visitatore	USA	Consent Mode v2 attivo dal 28/09/2026, in modalità base: tutte le categorie sono negate di default; GA4 si attiva, con anonimizzazione dell'IP, solo dopo che il visitatore concede il consenso "measurement". Non più senza condizioni. Data Privacy Framework/SCC (da confermare)	N — da ottenere/depositare (titolare)
Anthropic	Funzionalità AI	Prompt/contenuti inviati a Claude dalle funzionalità assistite da AI	USA (endpoint globale, nessuna regione UE configurata)	DPA + SCC + TIA; pianificato: regione UE su Vertex AI, zero-retention, Fase 1	N — da ottenere/depositare (titolare)
Meta (WhatsApp Business API, Facebook, Instagram)	Integrazioni di messaggistica collegate dal cliente	Contenuto dei messaggi e identificativi di contatto instradati dal cliente tramite le API di Meta	Dipende dal cliente	Autorizzato dal cliente; termini propri di Meta	N/A — collegato dal cliente

Nome	Servizio	Dati	Regione	Garanzia	DPA depositato
Telegram	Messaggistica bot collegata dal cliente	Contenuto dei messaggi e identificativi Telegram instradati dal cliente tramite il bot	Dipende dal cliente	Autorizzato dal cliente; termini propri di Telegram	N/A — collegato dal cliente
BulkGate	SMS	Numero di telefono del destinatario, contenuto del messaggio	Repubblica Ceca	DPA (UE-UE, nessun trasferimento previsto)	N — da ottenere/depositare (titolare)
Fathom	Trascrizioni chiamate e riepiloghi AI, collegato dal cliente	Registrazioni chiamate, trascrizioni, nomi dei partecipanti	USA	OAuth autorizzato dal cliente; DPA + SCC (da confermare)	N/A — collegato dal cliente; N per il DPA a livello piattaforma
Mapbox	Tile mappe	Coordinate di posizione mostrate nell'interfaccia; tipicamente nessun dato personale diretto	USA	DPA (da confermare)	N — da ottenere/depositare (titolare)
Apple / Google Wallet	Pass wallet	Nome del titolare della carta, identificativi carta/pass	USA	Termini standard di Apple/Google per emittenti pass	N — da ottenere/confermare (titolare)
Brave	Ricerca web per lo strumento "trova un dataset" del Copilot	Il testo della query di ricerca dell'utente, che può contenere dati personali digitati dall'utente	USA	DPA (da confermare)	N — da ottenere/depositare (titolare)
Chatwoot	Chat di supporto, self-hosted	Contenuto delle conversazioni di supporto, identificativi di contatto	Hetzner, Germania/Finlandia (UE/SEE)	Self-hosted, nessun trasferimento	N/A — non è un processor terzo (vedi nota Hetzner)
Zitadel	Identità/autenticazione, self-hosted	Identità di login, dati di sessione e permessi	Hetzner, Germania/Finlandia (UE/SEE)	Self-hosted, nessun trasferimento	N/A — non è un processor terzo (vedi nota Hetzner)
SigNoz	Osservabilità, self-hosted	Tracce/log/metriche, può includere metadati di richiesta	Hetzner, Germania/Finlandia (UE/SEE)	Self-hosted, nessun trasferimento	N/A — non è un processor terzo (vedi nota Hetzner)
Typesense / Postgres / Redis	Indice di ricerca / store relazionale / cache, self-hosted	Tutti i dati indicizzati e in cache della piattaforma	Hetzner, Germania/Finlandia (UE/SEE)	Self-hosted, nessun trasferimento	N/A — non è un processor terzo (vedi nota Hetzner)

Nome	Servizio	Dati	Regione	Garanzia	DPA depositato
mailinput.com	Verifica della deliverability delle email. La chiamata è stata rimossa dal codice della piattaforma il 05/11/2026; resta attiva in produzione fino al prossimo rilascio della piattaforma, dopodiché questa riga viene rimossa.	L'indirizzo email che l'utente sta digitando, inviato in tempo reale a terzi mentre digita	Sconosciuto — da verificare (titolare)	DPA (da confermare)	N — da ottenere/depositare (titolare)
Zoom	Solo prodotto Archimede, collegato dal cliente	Dati su riunione/partecipanti scambiati tra il workspace Archimede del cliente e Zoom	Dipende dal cliente	OAuth autorizzato dal cliente	N/A — collegato dal cliente
Integrazioni OAuth collegate dal cliente	GitHub, LinkedIn, Microsoft, HubSpot, Pipedrive, ClickUp, Fathom, GitLab, Sentry, Stripe, Airtable, PagerDuty, Klaviyo, Salesforce, Bitbucket, Mailchimp, Linear, Shopify	Ciò che l'account collegato dal cliente espone; i dati fluiscono solo quando il cliente collega l'integrazione	Dipende dal cliente	OAuth autorizzato dal cliente; termini propri di ciascun provider	N/A — collegato dal cliente

Le integrazioni dataset create dal cliente (blocchi di workflow che il cliente configura per chiamare un'API esterna) possono inviare dati agli host scelti dal cliente; questi host sono processor del cliente stesso, non sub-processor di Keix.

I dati inviati ai provider AI sono limitati al contenuto necessario alla funzionalità richiesta dall'utente. Esiste un opt-out contrattuale dall'uso di tale contenuto per l'addestramento dei modelli con i nostri attuali provider AI — da verificare (titolare) prima della pubblicazione di questa affermazione. L'elenco aggiornato dei sub-processor è pubblicato su keix.com/legal/sub-processors ed è anche disponibile su richiesta.

10. Protezione dei dati personali (GDPR)

- **Ruoli.** Per i dati trattati in piattaforma per conto dei clienti, Marketing Research Systems S.R.L. opera come **responsabile del trattamento** (processor) e il cliente è titolare. Per i dati di contatto commerciale, Marketing Research Systems S.R.L. è titolare autonomo.
- **Responsabile della protezione dei dati.** È in corso la nomina del Responsabile della protezione dei dati (DPO, art. 37 GDPR). Il DPO è contattabile all'indirizzo dpo@keix.com.
- **DPA.** Un modello di accordo sul trattamento dei dati (DPA, art. 28 GDPR), con i relativi allegati, è pronto ed è in revisione legale. Lo renderemo disponibile ai clienti al termine della revisione.
- **Diritti degli interessati.** Supportiamo richieste di accesso, rettifica, portabilità e cancellazione. L'esportazione di un workspace o di un account (un archivio ZIP con file JSON e CSV) fa parte del prodotto. Le richieste di cancellazione sono evase entro 30 giorni.
- **Cancellazione.** Il progetto della cancellazione automatica su tutti i sistemi è stato approvato il 05/11/2026. Il componente che la eseguirà è in sviluppo: gira nell'ambiente di sviluppo in una modalità che non cancella nulla e non è installato in produzione. Finché non sarà attivo, la propagazione della cancellazione su tutti i sistemi non è ancora automatica.
- **Conservazione.** Il 05/11/2026 è stata approvata una politica di conservazione che copre ogni categoria di dati personali. In base a essa, i contenuti dei workspace dei clienti sono cancellati su richiesta e comunque entro 30 giorni dalla fine del contratto. La cancellazione automatica viene introdotta una categoria di dati alla volta: oggi in produzione è attiva quella del registro degli accessi in lettura (12 mesi). La retention dei log applicativi è descritta al § 7. I dati di contatto commerciale sono conservati fino alla revoca del consenso.
- **Valutazione d'impatto.** Una valutazione d'impatto sulla protezione dei dati (DPIA) della piattaforma è in bozza.
- **Minimizzazione.** La piattaforma raccoglie solo i dati necessari alle funzionalità attivate dal cliente.

11. Gestione degli incidenti

- **Canale dedicato.** security@keix.com.
- **Processo formale.** Un piano di gestione degli incidenti e un runbook per le violazioni di dati, documentati, coprono classificazione per severità, contenimento, eradicazione, comunicazione ai clienti coinvolti senza ingiustificato ritardo e post-mortem documentato. Il piano è in bozza, in attesa di revisione del titolare/legale; è pianificata un'esercitazione tabletop annuale.
- **Notifiche regolatorie.** In caso di violazione di dati personali supportiamo i clienti negli obblighi di notifica (GDPR art. 33/34). Per i clienti soggetti a NIS2, i nostri impegni di notifica sono pensati per essere compatibili con le tempistiche di segnalazione ad ACN previste dall'art. 23 (preallarme entro 24 ore, notifica entro 72 ore).
- **Responsible disclosure.** I ricercatori di sicurezza possono segnalare vulnerabilità a security@keix.com. Ci impegniamo a dare riscontro entro 48 ore e un aggiornamento di stato entro 7 giorni. Non intraprendiamo azioni legali contro chi segnala in buona fede.

12. NIS2 — supporto alla supply chain dei clienti

Se la tua azienda è un soggetto essenziale o importante ai sensi della NIS2 (Dir. UE 2022/2555, recepita in Italia con il D.Lgs. 138/2024), l'art. 21 ti chiede di valutare la sicurezza dei tuoi fornitori ICT e di vincolarla per contratto. Per supportarti mettiamo a disposizione:

- questo whitepaper e risposte puntuali ai tuoi questionari di sicurezza;
- un modello di DPA (art. 28), pronto e in revisione legale, e un addendum contrattuale su notifica degli incidenti, requisiti minimi di sicurezza e diritti di audit, entrambi disponibili una volta finalizzati;
- l'audit trail nativo della piattaforma (event-sourcing) e il registro degli accessi in lettura, a supporto delle tue verifiche;
- l'impegno a notificarti tempestivamente qualsiasi incidente che riguardi i tuoi dati, coerente con i tuoi obblighi di notifica a 24/72 ore.

Documento aggiornato al: 2026-11-09 (v2.1). Per la versione più recente, il DPA o qualsiasi domanda: security@keix.com