KAIA-OR · WHITEPAPER · PRIVACY

Privacy by architecture

How KAIA-OR keeps sensitive evidence on the device, keeps each organization’s data separate, and makes sure that membership of a family or a workplace never becomes a way to look into other people’s lives.

DOCUMENT ID	WP-2
VERSION	1.0
DATE	3 November 2026
AUDIENCE	Privacy officers, data protection and legal teams, works councils, security architects, family organizers and individuals

Contents

1. Executive summary 3

2. Why security tools become surveillance, and our principles 4
   1. Three patterns 4
   2. Six principles 4

3. What stays on the device, and what an organization sees 6

4. Tenant isolation and membership 8
   1. Isolation between organizations 8
   2. Families 8
   3. Workplaces: for works councils and privacy officers 8

5. Cloud AI consent, authority and where data lives 10

6. How we test these properties, and questions to ask any vendor 11

7. What this means for you 12
   1. Glossary 12

© Kaia Technologies, Inc.

Executive summary

Security products ask for unusual trust. To tell you what affects your places and trips, a product seems to need to know where you are. To check a suspicious message, it seems to need to read it. To serve a family or a workplace, it seems to need to let someone look into other people's devices. Many products accept these trade-offs, and over time a security tool turns into a surveillance tool.

KAIA-OR is designed so that these trade-offs are unnecessary. Privacy is a property of the architecture, not a setting that can be quietly changed later. Six principles define it:

- **Local first.** Saved places, live position, checked messages and links, and topic preferences stay on the device. Matching and the assistant work on the device first, and questions reach a cloud AI service only with the person's own consent.
- **Consent before cloud AI.** Each person gives their own consent before anything is sent to a cloud AI service. Government organizations start with cloud AI off.
- **Membership is not access.** Roles manage membership, not people. Membership never grants access to another member's messages, devices, location or saved places.
- **Isolation between organizations.** Tenant isolation is enforced at the application layer, and each private operation is authorized for the tenant and the device.
- **AI informs, people decide.** Model output grants no authority.
- **Least data.** KAIA-OR collects only what a feature needs.

This paper explains each principle, what it means for individuals, families and organizations, and how we test that it holds. It closes with questions that any buyer can ask any vendor about privacy.

> ABOUT THIS PAPER
>
> This paper describes the design and the committed product scope of KAIA-OR at the level of principles and conceptual architecture. Capability availability depends on the edition and deployment. Contractual terms are set out in the KAIA-OR legal documents, which take precedence over this paper.

© Kaia Technologies, Inc.

1. Why security tools become surveillance, and our principles

Three patterns

Three common patterns turn protective tools into instruments of observation.

- **Location sharing as the core feature.** Many family products are built around seeing where members are. Once location is the product, each member's movements become visible to someone else, and opting out means leaving.
- **Inspection as the safety model.** Some products protect people by inspecting their messages, browsing or accounts on their behalf. The protection works only as long as someone else can see.
- **Employer reach into personal devices.** Workforce safety tools designed around the organization often extend into employees' personal phones. For travellers, the employer's program becomes the employer's view of where staff are.

Each pattern has a reasonable motive: a worried relative, a responsible employer. Each produces the same result. The person being protected loses control over information about themselves. In workplaces, this raises questions that works councils and privacy officers rightly ask. In families, it erodes trust between adults. Neither cost is necessary to deliver useful security.

The alternative is to put the protection where the person is. If events are matched to places on the device, nobody else needs to know the places. If a message is checked on the device, nobody else needs to read it. If each member of a family or an organization has their own KAIA-OR, nobody needs to look into anyone else's.

Six principles

THE PRINCIPLES, AND WHAT EACH ONE RULES OUT

Principle	What it means	What it rules out
Local first	Sensitive evidence and exact location stay on the device by default. Matching and the assistant work on the device first.	Central collection of where people are and what they check
Consent before cloud AI	Each person gives their own consent before anything is sent to a cloud AI service. Government organizations start with cloud AI off.	Silent use of a third-party AI service on personal content
Membership is not access	Roles manage membership, not people.	Owners or administrators reading members' messages, devices, location or saved places
Isolation between organizations	Tenant isolation is enforced at the application layer. Each private operation is authorized for the tenant and the device.	One organization's data reaching another organization
AI informs, people decide	Model output grants no authority. Agents act only within limits you set and with your authorization.	Automated decisions or actions taken on stale or unknown evidence

© Kaia Technologies, Inc.

Principle	What it means	What it rules out
Least data	KAIA-OR collects only what a feature needs.	Collecting data in case it becomes useful

The principles are deliberately simple. Each can be stated in one sentence and tested, and each holds whichever package a person uses, from Individual to Government.

© Kaia Technologies, Inc.

2. What stays on the device, and what an organization sees

The most useful privacy statement is a concrete one. The table below lists, item by item, where information stays and who can see it.

WHERE INFORMATION STAYS

Information	Where it stays	Who can see it
Saved places and trips	On your device	You
Live position	On your device, used for a nearby check and cleared when you stop	You
Messages and links you check	On your device	You
Questions to Hey KAIA	On your device; sent to a cloud AI service only with your consent	You
Topic preferences	On your device	You
Your alerts	On your device; notifications never name the place or the event	You
Organization sites, software and suppliers	In the organization's shared picture	The people the organization's roles allow
Membership and access records	In the organization's account	Its Owners and Administrators, through dated access reviews they can download and permission activity they can see

© Kaia Technologies, Inc.

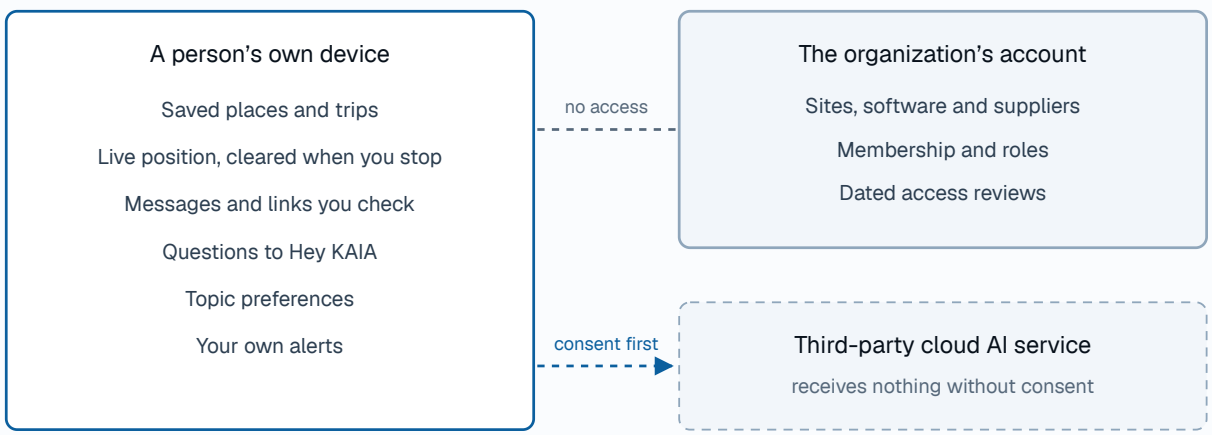


Figure 1. Where information stays. The figure is conceptual and names no service, vendor or infrastructure.

What an organization sees. Its own sites, software and suppliers, the events that touch them, and the membership of its own account. **What it does not see.** Its members' places, trips, whereabouts, messages, links, assistant questions or devices. The organization sees its sites, not its people's whereabouts.

Sharing is the member's choice. A member can choose to share their device's security status with a family owner or an organization administrator. The choice is made by the member, on the member's own device.

© Kaia Technologies, Inc.

3. Tenant isolation and membership

Isolation between organizations

Each organization in KAIA-OR is a separate tenant. Tenant isolation is enforced at the application layer. Authorization is mandatory at each private operation, not only at sign-in: before any private data is read or changed, the request must be authorized for the tenant and the device it comes from. A request that cannot be tied to the right tenant and device is refused. Where an integration is not configured, it fails closed and shows its real status, rather than falling back to a permissive default.

Two further rules keep authority narrow. Unknown or stale evidence cannot authorize an intervention. And no output from an AI model can widen what a person, a role or an agent is allowed to do. Isolation is therefore not only a boundary between organizations; it is also a boundary between what a request claims and what it is allowed to do.

Families

Each adult you invite, even when they live apart, gets their own KAIA-OR: their own places and trips, their own alerts and their own second look at messages and links, in English, French, Turkish or Hebrew. The family owner manages who is a member. Membership never grants access to another member's messages, devices, location or saved places. No one adds places on another member's behalf.

This is a deliberate choice about what a family product is for. A family is not served by one adult seeing where the others are. It is served by each adult having their own help, in their own language, on their own device. Roles manage membership, not people.

Workplaces: for works councils and privacy officers

Employers have legitimate responsibilities towards their sites and their people. Employees have a legitimate expectation that a workplace security product does not become a window into their personal lives. KAIA-OR draws the line in the architecture, so that it does not depend on a policy that could be changed.

WHAT AN EMPLOYER CAN AND CANNOT SEE

The employer can	The employer cannot
See its sites, software and suppliers, and the events that touch them	See where employees are, at work or abroad
Manage membership through roles	See employees' personal places or trips
Issue one-time invitations bound to an account	Read the messages or links employees check
Run and download dated access reviews, and see permission activity	Read the questions employees ask Hey KAIA
Send events into its own tools through the API and webhooks	Inspect employees' devices; an employee may choose to share their device's security status

© Kaia Technologies, Inc.

Travellers. Each traveller gets their own alerts for their own trips and sees what changed in the official travel advisory for their destination. The organization is not told where they are, and it does not follow their movements.

Questions a works council may ask. Can the employer see where I am? No. Can it read what I check? No. Can a manager add places to my KAIA-OR or see mine? No. Can the AI decide something about me? No: model output grants no authority, and decisions stay with people.

© Kaia Technologies, Inc.

4. Cloud AI consent, authority and where data lives

Cloud AI only with consent. Hey KAIA works on the device first. Some questions benefit from a larger cloud AI service. KAIA-OR never sends anything to a cloud AI service without explicit consent. Where one is used, it is a third-party AI service, and the person's own consent is asked, feature by feature, before anything is sent. Only that person can give it. Government organizations start with cloud AI off.

AI that cannot grant itself authority. An assistant that could grant itself access would be a way around the other principles in this paper. In KAIA-OR, model output grants no authority. Nothing a model produces can approve an action, change a permission or widen what an agent may do. Scanning agents act only within limits the person or organization sets, and only with authorization. No agent takes a destructive step, sends a message or makes a purchase without explicit authorization. The assistant is designed to resist instructions hidden in the content it reads, and social engineering aimed at the AI itself.

Where data lives: the choices you make. For individuals and families, the most important choice about where data lives is made by the architecture: sensitive personal evidence stays on the device by default. The remaining choices are explicit and belong to the person: whether to use cloud AI, and whether to share device status. For organizations, the shared picture holds what the organization itself enters (its sites, software and suppliers) and its membership records. An organization chooses the region where its shared data is held. Any further hosting requirements are raised with our team during evaluation and belong in the contract.

> LEAST DATA IN PRACTICE
>
> KAIA-OR does not need to know where you are to tell you what affects your places, because matching happens on your device. It does not need to read your messages centrally to give you a second look, because the check runs where the message already is. The less a central service holds, the less there is to expose.

© Kaia Technologies, Inc.

5. How we test these properties, and questions to ask any vendor

Privacy principles are only useful if they hold in practice. We describe our assurance at the level of practice, not internals.

- **Secure development practices,** with type checking and security tests as part of each release.
- **Pinned dependencies and supply-chain checks** before software is built and shipped.
- **Isolation tests.** Tenant and device authorization is exercised by automated isolation tests on each build, and is subject to independent review.
- **Evidence, not assertion.** A successful build is not a security result. Tests show that a property holds in the cases tested, and we describe them that way.
- **Reporting a vulnerability.** Security researchers can report a vulnerability through the contact on the KAIA-OR Trust page.

The questions below can be put to any vendor of family, workforce or personal security software, including us.

QUESTIONS TO ASK ANY VENDOR ABOUT PRIVACY

Ask	A strong answer
Where are my exact location and saved places processed and kept?	On my device, with the position cleared when I stop.
Can a family owner or an employer see members' messages, devices, location or places?	No. Membership is not access.
Is cloud AI used, and is consent asked before anything is sent?	Only with each person's own explicit consent, feature by feature.
Can AI output change permissions or trigger actions?	No. Authority comes only from people with the right role.
How is one organization's data kept apart from another's?	By tenant isolation, with authorization at each private operation, and tests that show it.
What does the organization see about travellers?	Its sites and the events that touch them, not where travellers are.
How do you describe the limits of your testing?	Plainly, as evidence for the cases tested, not as a promise.

© Kaia Technologies, Inc.

What this means for you

Individuals. Your places, your position and what you check stay on your device. Nothing goes to cloud AI unless you agree first.

Families. Each adult keeps their own KAIA-OR. The family owner manages membership, and membership never grants access to another member's messages, devices, location or saved places.

Organizations, works councils and privacy officers. The organization sees its sites, not its people's whereabouts. Access is accounted for through one-time invitations, dated access reviews that can be downloaded, and permission activity. Tenant isolation is enforced at the application layer.

Government organizations. Cloud AI starts off, and each person gives their own consent. Model output grants no authority, and scanning agents act only with your authorization. To evaluate KAIA-OR, request early access or choose Contact us on the KAIA-OR website.

Glossary

Term	Meaning in this paper
Tenant	One organization's separate space in KAIA-OR: its sites, software, suppliers and membership.
Tenant isolation	Keeping each tenant's data apart, enforced at the application layer by authorizing each private operation.
Local first	Processing and keeping sensitive evidence on the person's own device by default.
Membership	Belonging to a family or an organization in KAIA-OR. It never grants access to another member's data.
Cloud AI service	A third-party AI service that receives nothing without explicit consent.
Access review	A dated record of who has access to an organization's account, and with which role.

© Kaia Technologies, Inc.

WP-2 · Version 1.0 · 3 November 2026

Capability availability depends on the edition and deployment. Capabilities are described as the committed KAIA-OR product scope.