KAIA-OR · LIVRE BLANC · CONFIDENTIALITÉ

La confidentialité intégrée à l'architecture

Comment KAIA-OR garde les données probantes sensibles sur l'appareil, tient séparées les données de chaque organisation et veille à ce que l'appartenance à une famille ou à un milieu de travail ne devienne jamais un moyen de s'immiscer dans la vie d'autrui.

IDENTIFIANT DU DOCUMENT	WP-2
VERSION	1.0
DATE	3 novembre 2026
PUBLIC	Responsables de la protection des renseignements personnels, équipes de protection des données et équipes juridiques, représentants du personnel, architectes de sécurité, personnes qui gèrent un espace familial et particuliers

Table des matières

1. Sommaire 3

2. Pourquoi les outils de sécurité deviennent des outils de surveillance, et nos principes 4
   1. Trois schémas 4
   2. Six principes 4

3. Ce qui reste sur l'appareil, et ce que voit une organisation 6

4. Isolement des locataires et adhésion 8
   1. Isolement entre les organisations 8
   2. Familles 8
   3. Milieux de travail : à l'intention des représentants du personnel et des responsables de la protection des renseignements personnels 8

5. Consentement à l'IA infonuagique, autorité et lieu des données 10

6. Comment nous vérifions ces propriétés, et questions à poser à tout fournisseur 11

7. Ce que cela signifie pour vous 12
   1. Glossaire 12

© Kaia Technologies, Inc.

Sommaire

Les produits de sécurité demandent une confiance inhabituelle. Pour vous dire ce qui touche vos lieux et vos voyages, un produit semble devoir savoir où vous êtes. Pour vérifier un message suspect, il semble devoir le lire. Pour servir une famille ou un milieu de travail, il semble devoir permettre à quelqu'un de regarder dans les appareils d'autres personnes. Beaucoup de produits acceptent ces compromis et, avec le temps, l'outil de sécurité devient un outil de surveillance.

KAIA-OR est conçu pour rendre ces compromis inutiles. La confidentialité est une propriété de l'architecture, et non un paramètre qu'on pourrait modifier discrètement plus tard. Six principes la définissent :

- **Local d'abord.** Les lieux enregistrés, la position en direct, les messages et les liens vérifiés ainsi que les préférences de sujets restent sur l'appareil. La mise en correspondance et l'assistant fonctionnent d'abord sur l'appareil, et les questions ne parviennent à un service d'IA infonuagique qu'avec le consentement de la personne elle-même.
- **Consentement avant toute IA infonuagique.** Chaque personne donne elle-même son consentement avant que quoi que ce soit soit transmis à un service d'IA infonuagique. Pour les organismes gouvernementaux, l'IA infonuagique est désactivée au départ.
- **Être membre ne donne pas accès.** Les rôles gèrent l'adhésion, pas les personnes. L'adhésion ne donne jamais accès aux messages, aux appareils, à la position ni aux lieux enregistrés d'un autre membre.
- **Isolement entre les organisations.** L'isolement des locataires est appliqué dans la couche applicative, et chaque opération privée est autorisée pour le locataire et pour l'appareil.
- **L'IA informe, les personnes décident.** Les résultats produits par le modèle n'accordent aucune autorité.
- **Le minimum de données.** KAIA-OR ne recueille que ce dont une fonctionnalité a besoin.

Ce livre blanc explique chaque principe, ce qu'il signifie pour les particuliers, les familles et les organisations, et la façon dont nous vérifions qu'il tient. Il se termine par des questions que tout acheteur peut poser à tout fournisseur au sujet de la confidentialité.

> **À PROPOS DE CE LIVRE BLANC**
>
> Ce livre blanc décrit la conception et la portée engagée du produit KAIA-OR au niveau des principes et de l'architecture conceptuelle. La disponibilité des fonctionnalités dépend du forfait et du déploiement. Les modalités contractuelles sont énoncées dans les documents juridiques de KAIA-OR, qui ont préséance sur ce livre blanc.

© Kaia Technologies, Inc.

1. Pourquoi les outils de sécurité deviennent des outils de surveillance, et nos principes

Trois schémas

Trois schémas courants transforment des outils de protection en instruments d'observation.

- **Le partage de position comme fonction centrale.** Beaucoup de produits familiaux sont conçus pour voir où se trouvent les membres. Dès que la position devient le produit, les déplacements de chaque membre deviennent visibles pour quelqu'un d'autre, et s'y soustraire signifie partir.
- **L'inspection comme modèle de sécurité.** Certains produits protègent les gens en inspectant leurs messages, leur navigation ou leurs comptes à leur place. La protection ne fonctionne que tant que quelqu'un d'autre peut voir.
- **La portée de l'employeur jusque dans les appareils personnels.** Les outils de sécurité du personnel conçus autour de l'organisation s'étendent souvent aux téléphones personnels du personnel. Pour les personnes en déplacement, le programme de l'employeur devient la vue de l'employeur sur l'endroit où se trouve son personnel.

Chaque schéma part d'une intention raisonnable : un proche inquiet, un employeur responsable. Chacun produit le même résultat : la personne protégée perd le contrôle de l'information qui la concerne. En milieu de travail, cela soulève des questions que les représentants du personnel et les responsables de la protection des renseignements personnels ont raison de poser. Dans les familles, cela mine la confiance entre adultes. Aucun de ces coûts n'est nécessaire pour offrir une sécurité utile.

L'autre voie consiste à placer la protection là où se trouve la personne. Si les événements sont mis en correspondance avec les lieux sur l'appareil, personne d'autre n'a besoin de connaître ces lieux. Si un message est vérifié sur l'appareil, personne d'autre n'a besoin de le lire. Si chaque membre d'une famille ou d'une organisation a son propre KAIA-OR, personne n'a besoin de regarder dans celui des autres.

Six principes

LES PRINCIPES, ET CE QUE CHACUN EXCLUT

Principe	Ce qu'il signifie	Ce qu'il exclut
Local d'abord	Par défaut, les données probantes sensibles et la position exacte restent sur l'appareil. La mise en correspondance et l'assistant fonctionnent d'abord sur l'appareil.	La collecte centralisée de l'endroit où se trouvent les gens et de ce qu'ils vérifient
Consentement avant toute IA infonuagique	Chaque personne donne elle-même son consentement avant que quoi que ce soit soit transmis à un service d'IA infonuagique. Pour les organismes gouvernementaux, l'IA infonuagique est désactivée au départ.	L'utilisation, à l'insu de la personne, d'un service d'IA tiers sur du contenu personnel

© Kaia Technologies, Inc.

Principe	Ce qu'il signifie	Ce qu'il exclut
Être membre ne donne pas accès	Les rôles gèrent l'adhésion, pas les personnes.	La lecture, par les personnes ayant le rôle Propriétaire ou Administrateur, des messages, des appareils, de la position ou des lieux enregistrés des membres
Isolement entre les organisations	L'isolement des locataires est appliqué dans la couche applicative. Chaque opération privée est autorisée pour le locataire et pour l'appareil.	Les données d'une organisation qui parviennent à une autre organisation
L'IA informe, les personnes décident	Les résultats produits par le modèle n'accordent aucune autorité. Les agents agissent uniquement dans les limites que vous fixez et avec votre autorisation.	Les décisions ou les actions automatisées fondées sur des données probantes non actualisées ou inconnues
Le minimum de données	KAIA-OR ne recueille que ce dont une fonctionnalité a besoin.	La collecte de données au cas où elles deviendraient utiles

Les principes sont volontairement simples. Chacun peut être énoncé en une phrase et vérifié, et chacun s'applique quel que soit le forfait utilisé, d'Individuel à Gouvernement.

© Kaia Technologies, Inc.

2. Ce qui reste sur l’appareil, et ce que voit une organisation

L’énoncé de confidentialité le plus utile est un énoncé concret. Le tableau ci-dessous indique, élément par élément, où l’information reste et qui peut la voir.

OÙ L’INFORMATION RESTE

Information	Où elle reste	Qui peut la voir
Lieux enregistrés et voyages	Sur votre appareil	Vous
Position en direct	Sur votre appareil, utilisée pour une vérification des environs et effacée lorsque vous arrêtez	Vous
Messages et liens que vous vérifiez	Sur votre appareil	Vous
Questions posées à Hey KAIA	Sur votre appareil; transmises à un service d’IA infonuagique seulement avec votre consentement	Vous
Préférences de sujets	Sur votre appareil	Vous
Vos alertes	Sur votre appareil; les notifications ne nomment jamais le lieu ni l’événement	Vous
Sites, logiciels et fournisseurs de l’organisation	Dans l’image commune de l’organisation	Les personnes autorisées par les rôles de l’organisation
Registres d’adhésion et d’accès	Dans le compte de l’organisation	Les personnes ayant le rôle Propriétaire ou Administrateur, au moyen des revues des accès datées qu’elles peuvent télécharger et de l’activité des autorisations qu’elles peuvent consulter

© Kaia Technologies, Inc.

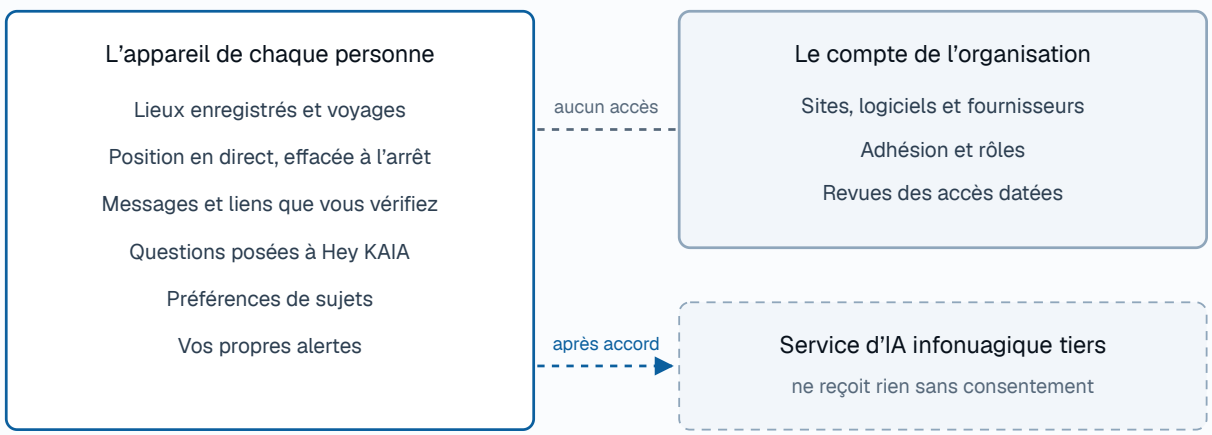


Figure 1. Où l’information reste. La figure est conceptuelle et ne nomme aucun service, fournisseur ni infrastructure.

Ce que voit une organisation. Ses propres sites, logiciels et fournisseurs, les événements qui les touchent et l’adhésion à son propre compte. **Ce qu’elle ne voit pas.** Les lieux, les voyages, les allées et venues, les messages, les liens, les questions à l’assistant ou les appareils de ses membres. L’organisation voit ses sites, et non l’endroit où se trouvent ses membres.

Le partage relève du choix du membre. Un membre peut choisir de partager l’état de sécurité de son appareil avec la personne propriétaire de sa famille ou une personne ayant le rôle Administrateur dans son organisation. Ce choix est fait par le membre, sur son propre appareil.

© Kaia Technologies, Inc.

3. Isolement des locataires et adhésion

Isolement entre les organisations

Dans KAIA-OR, chaque organisation est un locataire distinct. L'isolement des locataires est appliqué dans la couche applicative. L'autorisation est obligatoire à chaque opération privée, et pas seulement à la connexion : avant que des données privées soient lues ou modifiées, la demande doit être autorisée pour le locataire et pour l'appareil dont elle provient. Une demande qui ne peut pas être rattachée au bon locataire et au bon appareil est refusée. Lorsqu'une intégration n'est pas configurée, elle échoue en mode fermé et affiche son état réel, plutôt que de se rabattre sur un réglage permissif par défaut.

Deux autres règles restreignent l'autorité. Des données probantes inconnues ou non actualisées ne peuvent pas autoriser une intervention. Et aucun résultat d'un modèle d'IA ne peut élargir ce qu'une personne, un rôle ou un agent est autorisé à faire. L'isolement n'est donc pas seulement une frontière entre les organisations; c'est aussi une frontière entre ce qu'une demande prétend et ce qu'elle est autorisée à faire.

Familles

Chaque adulte que vous invitez, même s'il ne vit pas sous votre toit, obtient son propre KAIA-OR : ses propres lieux et voyages, ses propres alertes et son propre second regard sur les messages et les liens, en anglais, en français, en turc ou en hébreu. La personne propriétaire de la famille gère qui en est membre. L'adhésion ne donne jamais accès aux messages, aux appareils, à la position ni aux lieux enregistrés d'un autre membre. Personne n'ajoute de lieux au nom d'un autre membre.

C'est un choix délibéré quant à la raison d'être d'un produit familial. Une famille n'est pas bien servie lorsqu'un adulte voit où se trouvent les autres. Elle l'est lorsque chaque adulte dispose de sa propre aide, dans sa propre langue, sur son propre appareil. Les rôles gèrent l'adhésion, pas les personnes.

Milieux de travail : à l'intention des représentants du personnel et des responsables de la protection des renseignements personnels

Les employeurs ont des responsabilités légitimes envers leurs sites et leur personnel. Le personnel s'attend légitimement à ce qu'un produit de sécurité en milieu de travail ne devienne pas une fenêtre sur sa vie personnelle. KAIA-OR trace cette limite dans l'architecture, de sorte qu'elle ne dépende pas d'une politique qui pourrait changer.

CE QUE L'EMPLOYEUR PEUT VOIR, ET CE QU'IL NE PEUT PAS VOIR

L'employeur peut	L'employeur ne peut pas
Voir ses sites, ses logiciels et ses fournisseurs, et les événements qui les touchent	Voir où se trouvent les membres du personnel, au travail ou à l'étranger
Gérer l'adhésion au moyen des rôles	Voir les lieux personnels ou les voyages du personnel
Émettre des invitations à usage unique liées à un compte	Lire les messages ou les liens que le personnel vérifie
Effectuer et télécharger des revues des accès datées, et consulter l'activité des autorisations	Lire les questions que le personnel pose à Hey KAIA

© Kaia Technologies, Inc.

L’employeur peut	L’employeur ne peut pas
Transmettre les événements à ses propres outils au moyen de l’API et de crochets Web (webhooks)	Inspecter les appareils du personnel; un membre du personnel peut choisir de partager l’état de sécurité de son appareil

Personnes en déplacement. Chaque personne en déplacement reçoit ses propres alertes pour ses propres voyages et voit ce qui a changé dans les conseils officiels aux voyageurs pour sa destination. L’organisation n’est pas informée de l’endroit où elle se trouve et ne suit pas ses déplacements.

Questions que les représentants du personnel peuvent poser. L’employeur peut-il voir où je suis? Non. Peut-il lire ce que je vérifie? Non. Un gestionnaire peut-il ajouter des lieux à mon KAIA-OR ou voir les miens? Non. L’IA peut-elle prendre une décision à mon sujet? Non : les résultats produits par le modèle n’accordent aucune autorité, et les décisions restent entre les mains des personnes.

© Kaia Technologies, Inc.

4. Consentement à l'IA infonuagique, autorité et lieu des données

L'IA infonuagique, seulement avec consentement. Hey KAIA fonctionne d'abord sur l'appareil. Certaines questions gagnent à être confiées à un service d'IA infonuagique de plus grande envergure. KAIA-OR ne transmet jamais rien à un service d'IA infonuagique sans consentement exprès. Lorsqu'un tel service est utilisé, il s'agit d'un service d'IA tiers, et le consentement de la personne elle-même est demandé, fonction par fonction, avant toute transmission. Seule cette personne peut le donner. Pour les organismes gouvernementaux, l'IA infonuagique est désactivée au départ.

Une IA qui ne peut pas s'accorder d'autorité. Un assistant qui pourrait s'accorder lui-même des accès permettrait de contourner les autres principes de ce livre blanc. Dans KAIA-OR, les résultats produits par le modèle n'accordent aucune autorité. Rien de ce que produit un modèle ne peut approuver une action, modifier une autorisation ou élargir ce qu'un agent peut faire. Les agents d'exploration agissent uniquement dans les limites que fixe la personne ou l'organisation, et seulement avec autorisation. Aucun agent ne prend de mesure destructive, n'envoie de message ni n'effectue d'achat sans autorisation expresse. L'assistant est conçu pour résister aux instructions dissimulées dans le contenu qu'il lit, ainsi qu'à l'ingénierie sociale visant l'IA elle-même.

Le lieu des données : les choix que vous faites. Pour les particuliers et les familles, le choix le plus important quant au lieu des données est fait par l'architecture : par défaut, les données probantes personnelles sensibles restent sur l'appareil. Les autres choix sont explicites et appartiennent à la personne : utiliser ou non l'IA infonuagique, et partager ou non l'état de son appareil. Pour les organisations, l'image commune contient ce que l'organisation saisit elle-même (ses sites, ses logiciels et ses fournisseurs) et ses registres d'adhésion. Chaque organisation choisit la région où sont conservées ses données partagées. Toute autre exigence d'hébergement est présentée à notre équipe pendant l'évaluation et relève du contrat.

> **LE MINIMUM DE DONNÉES EN PRATIQUE**
>
> KAIA-OR n'a pas besoin de savoir où vous êtes pour vous dire ce qui touche vos lieux, parce que la mise en correspondance se fait sur votre appareil. Il n'a pas besoin de lire vos messages de façon centralisée pour vous offrir un second regard, parce que la vérification s'effectue là où le message se trouve déjà. Moins un service central détient de données, moins il y a à exposer.

© Kaia Technologies, Inc.

5. Comment nous vérifions ces propriétés, et questions à poser à tout fournisseur

Des principes de confidentialité ne sont utiles que s'ils tiennent en pratique. Nous décrivons notre assurance au niveau des pratiques, et non des mécanismes internes.

- **Des pratiques de développement sécurisé,** avec vérification des types et tests de sécurité à chaque version.
- **Des dépendances épinglées et des vérifications de la chaîne d'approvisionnement** avant que le logiciel soit compilé et livré.
- **Des tests d'isolement.** L'autorisation par locataire et par appareil est éprouvée par des tests d'isolement automatisés à chaque compilation, et fait l'objet d'un examen indépendant.
- **Des données probantes, pas des affirmations.** Une compilation réussie n'est pas un résultat de sécurité. Les tests montrent qu'une propriété tient dans les cas testés, et nous les décrivons ainsi.
- **Signaler une vulnérabilité.** Les personnes qui font de la recherche en sécurité peuvent signaler une vulnérabilité au moyen des coordonnées indiquées à la page Confiance de KAIA-OR.

Les questions ci-dessous peuvent être posées à tout fournisseur de logiciels de sécurité familiale, de sécurité du personnel ou de sécurité personnelle, y compris nous.

QUESTIONS À POSER À TOUT FOURNISSEUR AU SUJET DE LA CONFIDENTIALITÉ

Question	Une réponse solide
Où ma position exacte et mes lieux enregistrés sont-ils traités et conservés?	Sur mon appareil, et la position est effacée lorsque j'arrête.
La personne propriétaire d'une famille ou un employeur peut-il voir les messages, les appareils, la position ou les lieux des membres?	Non. Être membre ne donne pas accès.
L'IA infonuagique est-elle utilisée, et le consentement est-il demandé avant toute transmission?	Seulement avec le consentement exprès de chaque personne, fonction par fonction.
Les résultats de l'IA peuvent-ils modifier des autorisations ou déclencher des actions?	Non. L'autorité vient seulement des personnes qui ont le rôle approprié.
Comment les données d'une organisation sont-elles tenues à l'écart de celles d'une autre?	Par l'isolement des locataires, avec une autorisation à chaque opération privée, et des tests qui le démontrent.
Que voit l'organisation au sujet des personnes en déplacement?	Ses sites et les événements qui les touchent, et non l'endroit où se trouvent ces personnes.
Comment décrivez-vous les limites de vos tests?	Clairement, comme des données probantes pour les cas testés, et non comme une promesse.

© Kaia Technologies, Inc.

Ce que cela signifie pour vous

Particuliers. Vos lieux, votre position et ce que vous vérifiez restent sur votre appareil. Rien n'est transmis à l'IA infonuagique sans votre accord préalable.

Familles. Chaque adulte garde son propre KAIA-OR. La personne propriétaire de la famille gère l'adhésion, et l'adhésion ne donne jamais accès aux messages, aux appareils, à la position ni aux lieux enregistrés d'un autre membre.

Organisations, représentants du personnel et responsables de la protection des renseignements personnels. L'organisation voit ses sites, et non l'endroit où se trouvent ses membres. Les accès sont consignés au moyen d'invitations à usage unique, de revues des accès datées qui peuvent être téléchargées et de l'activité des autorisations. L'isolement des locataires est appliqué dans la couche applicative.

Organismes gouvernementaux. L'IA infonuagique est désactivée au départ, et chaque personne donne elle-même son consentement. Les résultats produits par le modèle n'accordent aucune autorité, et les agents d'exploration agissent uniquement avec votre autorisation. Pour évaluer KAIA-OR, demandez un accès anticipé ou choisissez Nous joindre sur le site Web de KAIA-OR.

Glossaire

Terme	Sens dans ce livre blanc
Locataire	L'espace distinct d'une organisation dans KAIA-OR : ses sites, ses logiciels, ses fournisseurs et ses membres.
Isolement des locataires	Le fait de tenir séparées les données de chaque locataire, appliqué dans la couche applicative par l'autorisation de chaque opération privée.
Local d'abord	Le traitement et la conservation, par défaut, des données probantes sensibles sur l'appareil de la personne elle-même.
Adhésion	L'appartenance à une famille ou à une organisation dans KAIA-OR. Elle ne donne jamais accès aux données d'un autre membre.
Service d'IA infonuagique	Un service d'IA tiers qui ne reçoit rien sans consentement exprès.
Revue des accès	Un registre daté des personnes qui ont accès au compte d'une organisation, et avec quel rôle.

© Kaia Technologies, Inc.

WP-2 · Version 1.0 · 3 novembre 2026

La disponibilité des fonctionnalités dépend du forfait et du déploiement. Les fonctionnalités décrites correspondent à la portée engagée du produit KAIA-OR.