

K SCAN AI

Privacy Policy

Full public policy for the website and K Scan AI mobile applications

Effective Date: June 12, 2026 | Last Updated: August 24, 2026 | Contact: kscanai.app@gmail.com

Governing full HTML version: <https://kscan.app/legal/privacy>

Public summary: <https://kscan.app/privacy>

K Scan AI ("K Scan AI," "we," "our," or "us") respects your privacy. This Privacy Policy explains how we collect, use, disclose, retain, and protect information when you use the K Scan AI website, Android and iOS mobile applications, APIs, AI systems, Elise and her StyleChat conversational capability, Scanner, Recent Scans, Closet and saved style content, Saved Looks, Dressing Rooms, shopping-assistance tools, and related services (collectively, the "Service").

K Scan AI is a fashion-specific visual discovery, style-assistance, and shopping-assistance service. K Scan AI mobile applications are available through Google Play and the Apple App Store. Depending on the platform and feature used, users may scan or select fashion-related images, receive AI-generated item and style results, view retailer-neutral shopping options, save fashion content, use Elise for conversational styling support, receive optional spoken stylist responses, organize or share items through Dressing Rooms, and use optional weather-aware styling context.

This Policy describes the current Service as of the Last Updated date. Website, investor, demonstration, prototype, or roadmap materials may describe planned functionality. Planned functionality is not treated as active data processing unless it is enabled in the Service and described here.

Privacy Controls Summary

- K Scan AI is intended for users 18 years of age and older. The Service is not directed to children or minors.
- Camera and image-picker access are used only when you choose to capture or select fashion-related images.
- The mobile scan flow may support selecting and reviewing up to five images before submission and may identify multiple garments across those images.
- On supported photo-library or gallery upload flows, K Scan AI may prepare a new image copy on your device before analysis by resizing or re-encoding the image and removing source metadata that is not needed for the Service. This preparation does not itself provide face or license-plate masking and is not guaranteed across every image path unless separately disclosed.
- K Scan AI does not currently have active local face detection, automatic face blurring, automatic bystander masking, or automatic license-plate masking on the connected mobile upload path. Avoid submitting sensitive or non-fashion content.
- K Scan AI is not designed for surveillance, facial recognition, biometric identification, or identifying people. K Scan AI does not create or retain biometric templates, faceprints, face geometry, or identity profiles.
- Images, prompts, Elise messages, style context, and related information may be processed through K Scan AI cloud systems and authorized AI or infrastructure providers. The Service is not device-only or cloud-free.
- Elise may use a bounded recent conversation window, authorized fashion content that you select or reference, and non-sensitive style preferences to personalize responses. K Scan AI is designed not to infer sensitive personal traits from your photographs, wardrobe, name, or voice.
- Elise spoken responses use text-to-speech. The feature does not record your voice, and the mobile apps do not request microphone permission for Elise spoken responses.
- Recent Scans and their saved shopping snapshots are device-local by default. Cloud Saved Scans synchronization is disabled by default. Account-backed Closet, Style Library, Dressing Room, Shared with Me, and related content may use cloud services where the feature is enabled.
- The mobile apps may request foreground location for optional weather-aware styling. Depending on platform and operating-system settings, you may be able to control the precision of the permission you grant. For weather-aware styling, K Scan AI uses approximate, rounded location context rather than storing raw precise GPS coordinates, and K Scan AI does not use background location for this feature.
- K Scan AI does not currently use third-party advertising SDKs or collect Advertising ID for targeted advertising.
- When an account-deletion request is accepted, K Scan AI deactivates the account and uses a limited restoration period of approximately 30 days. If the account is not restored and no legal, security, or technical hold applies, it becomes eligible for permanent deletion. Deletion is not an instantaneous erase operation.
- Dressing Room safety controls include in-app report-message, report-user, and block-user functions. Blocking is enforced across relevant authorization surfaces.

- AI-generated responses can be reported in-app. The report is designed to store structured moderation information and limited allowlisted identifiers or context rather than the raw AI response, uploaded photos, scan media, or raw image content.
- Mirror Selfie may use user-requested image and pose/body-positioning processing for the fashion experience. It is not used for facial recognition, biometric identification, or creating identity profiles.

1. Scope and Overview

This Policy applies to the K Scan AI website, Android and iOS mobile applications available through Google Play and the Apple App Store, APIs, AI systems, and related services unless a separate privacy notice applies. It covers information you provide, information generated through use of the Service, information stored locally on your device, information stored in K Scan AI cloud systems, and information processed by authorized service providers.

K Scan AI distributes its mobile applications through Google Play and the Apple App Store. Google Play Data Safety disclosures, Apple App Privacy disclosures, and in-app disclosures should be read together with this Policy. If a feature materially changes data collection or processing, K Scan AI will update this Policy and required platform disclosures before or when the change is enabled.

2. Age Eligibility and 18+ Audience

K Scan AI is intended for users 18 years of age and older. The Service is not directed to children or minors, and users under 18 should not use the Service.

K Scan AI does not knowingly collect personal information from children or minors. If we learn that we collected information from a person under 18, we will take reasonable steps to delete or restrict it, subject to legal, safety, security, fraud-prevention, backup, and technical requirements. K Scan AI does not participate in Google Play Families or Designed for Families.

3. Key Definitions

Personal Information or Personal Data: Information that identifies, relates to, describes, can reasonably be linked to, or could reasonably identify an individual or household.

User Content: Content a user submits, captures, uploads, saves, sends, or shares through the Service, including images, scan content, Elise or StyleChat messages, room content, notes, captions, and support communications.

Submitted Visual Data: Camera captures, selected photos, screenshots, prepared image derivatives, and other visual inputs submitted for fashion scanning, item recognition, style analysis, shopping assistance, Closet or Style Library features, Recent Scans, Saved Looks, Dressing Rooms, or Elise.

Prepared Image: A new image derivative that K Scan AI may create locally on supported upload flows by resizing or re-encoding a selected image and removing source metadata that is not needed for the requested feature. A Prepared Image does not mean face or license-plate masking has occurred.

Derived Fashion Data: Information generated from Submitted Visual Data or use of the Service, such as garment category, subtype, brand evidence, color, texture, pattern, material estimate, silhouette, fit, visible construction details, product-match signals, source-image association, shopping queries, and other fashion-related analytical outputs.

Elise: K Scan AI's AI stylist interface. StyleChat is Elise's conversational capability. Elise may provide text responses and, when enabled and available, generated spoken responses.

Styling Preferences and Signature Style: User-provided or non-sensitive fashion preferences used to personalize Elise, including feedback such as Helpful or Not My Style, optional styling-context choices, and fashion preferences derived from authorized items and interactions. Some preference or feedback details may remain device-local while compact or account-backed fashion summaries may be used by Elise.

Recent Scans: Saved scan records and related commerce snapshots stored on the user's device by default, including available retailer, price, currency, product link, and product-image information captured when the scan is saved.

Dressing Rooms: Account-backed private or shared spaces used to organize, discuss, save, and share fashion-related items and images.

Safety and Moderation Data: Block relationships, report categories, target user or content identifiers, room or message identifiers, AI-response report identifiers, timestamps, status information, and limited context used to investigate safety, abuse, policy, or moderation issues.

Approximate Location Data: Coarse or rounded location information used for optional weather-aware styling, localization, security, fraud prevention, or service delivery. The current weather-aware styling path does not require K Scan AI to store raw precise GPS coordinates.

Account Deletion Lifecycle: The staged process in which a valid deletion request deactivates the account, allows a limited restoration period, and, if not restored and no hold applies, makes the account eligible for verified permanent deletion.

Mirror Selfie: A user-requested visual experience that may use image and pose/body-positioning signals to support fashion visualization. It is not a facial-recognition, identity-verification, or biometric-identification feature.

Aggregated or De-identified Data: Information processed or combined so that it does not reasonably identify a person and is subject to controls designed to prevent re-identification.

4. Information We Collect

4.1 Account, Contact, Authentication, and Stylist Preference Information

We may collect information you provide directly, including your name if provided, email address, profile settings, support messages, feedback, privacy requests, and other account information. Authentication may be provided through email, Google, Apple, or another enabled provider. We receive only the profile and authentication information permitted by the provider and your settings.

K Scan AI may also store account-scoped stylist preferences, such as the stylist or avatar you select, a stylist display name, and an optional self-disclosed styling-context preference such as man, woman, or prefer not to say where that feature is enabled. K Scan AI uses this as styling context and does not infer it from your photographs, name, voice, Closet contents, scans, or Dressing Rooms.

4.2 Camera, Image Picker, Multi-Image Scan, and Local Image Preparation

When you intentionally start a scan or select images, K Scan AI may access the camera or the images you select through the operating-system image picker. The mobile scan flow may support selecting and reviewing between one and five images before submission. You can remove selected images before starting analysis.

On supported photo-library or gallery upload paths, K Scan AI may create a new image copy on your device before remote analysis. This preparation may resize or re-encode the selected image as a fresh JPEG derivative and remove source metadata, such as metadata that is not needed to provide the requested fashion feature. Temporary prepared copies may be deleted after use. K Scan AI does not claim that every possible image path uses the same preparation unless that path has been separately verified and disclosed.

Submitted Visual Data may be resized, compressed, transmitted through encrypted connections, and processed by K Scan AI cloud services and authorized AI providers. A scan may produce one result, multiple garment results, partial results, or no result. K Scan AI may maintain an association between each detected item and its source image so that results, saved items, shopping options, and Dressing Room actions remain understandable.

Camera access is activated only when you initiate a camera action. K Scan AI does not use the camera for continuous monitoring, background capture, or surveillance.

K Scan AI does not currently have active local face detection, automatic face blurring, automatic bystander masking, automatic license-plate detection, or automatic license-plate masking on the applicable mobile upload path. Local metadata stripping or image re-encoding is not the same as face or license-plate masking. If an image contains a face, bystander, license plate, private document, or other identifying visual element, that element may be included in the image transmitted for remote analysis. Do not submit sensitive or non-fashion content unless you intend that content to be processed as part of your request.

When you use Mirror Selfie, K Scan AI may process the image and pose/body-positioning information needed to provide the requested fashion experience. K Scan AI does not use Mirror Selfie to identify you, perform facial recognition, authenticate identity, or create biometric identity profiles.

4.3 Device-Local Recent Scans and Commerce Snapshots

Recent Scans are stored on the device by default. When you save a scan that contains shopping options, K Scan AI may store a snapshot of the available retailer, source, price, currency, product link, availability, product type, and product image information. Reopening a saved scan uses that stored snapshot. If no shopping option existed when the scan was saved, none may appear when it is reopened.

Cloud Saved Scans synchronization is disabled by default. Device-local records do not automatically become available on another device. Clearing app data or uninstalling the app may remove device-local records. Account deletion from K Scan AI cloud systems may not erase a local copy that remains on a disconnected device; you may also delete local records through the app, clear app data, or uninstall the app.

4.4 Closet, Style Library, Saved Looks, and Account-Backed Content

When you save, own, upload, organize, or attach content to account-backed features, K Scan AI may store the content and related metadata in private cloud storage associated with your account. Depending on the feature, this may include selected images, inspiration uploads, Closet or wardrobe item information, Saved Look information, item metadata, style preferences, timestamps, ownership or relationship status, and references needed to display, organize, retrieve, authorize, or delete the content. Signed or time-limited URLs may be generated to display protected images.

4.5 Elise, StyleChat, Signature Style, Style Preferences, and Spoken Responses

When you use Elise or her StyleChat conversational capability, K Scan AI may process and persist your prompts and messages, selected item or image context, references to authorized K Scan AI content, recent conversation context, saved styling preferences, and technical session information needed to provide the feature. Persisted conversation history may be associated with your account so you can reopen it.

For generating a new Elise response, K Scan AI may provide the AI model with a bounded recent conversation window rather than your entire lifetime conversation archive. The current styling architecture may also provide a fashion-oriented summary of items you intentionally reference or that are authorized for the current context, such as garment type, brand, color, material, pattern, silhouette, fit, construction details, identification confidence, and whether an item is owned, scanned, saved, or shared.

Elise may use authorized information from your Closet, Style Library, Saved Looks, or Dressing Rooms when you invoke Elise from that context or intentionally attach or reference those items. K Scan AI does not describe Elise as automatically reading every Dressing Room message or every piece of account content without a feature context or authorization path.

K Scan AI may use non-sensitive fashion preferences to personalize Elise. This may include feedback such as Helpful or Not My Style; compact feedback summaries; commonly selected brands, clothing categories, colors, or general price ranges derived from authorized fashion activity; and optional self-disclosed styling context. Some detailed feedback reasons and preference controls may remain stored only on your device, while compact summaries or account-backed fashion preference signals may be used by the Service. K Scan AI does not use these systems to infer sensitive personal characteristics such as race, religion, health conditions, disability, sexual orientation, biometric identity, age, or body measurements.

You can voluntarily type sensitive information into a free-text message. Please do not provide sensitive personal information, health information, financial information, government identification, authentication secrets, or private information about other people unless it is necessary for the feature you are using and you have the right to provide it.

When weather-aware styling is enabled and you grant location permission, Elise may receive rounded approximate location context and resulting local weather information as described in Section 4.8. Raw precise GPS coordinates are not stored for the current weather-aware styling feature.

When Spoken Responses are enabled, K Scan AI may send the text of an eligible Elise response, limited message and session identifiers, and the selected stylist voice profile to K Scan AI's speech service and an authorized text-to-speech provider, currently ElevenLabs, to generate audio and timing information. Generated audio may be cached temporarily on the device for playback and removed after playback, interruption, or cache cleanup.

Spoken Responses do not record your voice. The mobile apps do not request microphone permission for Elise spoken responses, do not collect raw microphone audio through that feature, and do not create voiceprints or biometric voice identifiers. Spoken Responses may be unavailable because of network conditions, provider availability, account limits, or provider quota.

4.6 Dressing Rooms, Shared with Me, Messaging, Sharing, and Safety

Owned Dressing Rooms, room items, and Shared with Me memberships are account-backed. K Scan AI may process room names, descriptions, item snapshots, images, participants, membership status, messages, reactions, timestamps, invitations, removals, revocations, and related metadata to operate these features.

Content you deliberately add to a shared Dressing Room may be visible to room members. Where a room owner enables a share link or public preview, selected room details, items, and images may be visible to anyone who possesses the active link. Share links and memberships may be revoked, but recipients may retain screenshots or copies of content they previously viewed. K Scan AI does not describe Dressing Rooms as end-to-end encrypted or zero-knowledge storage.

K Scan AI processes block relationships and moderation reports to enforce user-safety boundaries. A blocked or departed participant may lose collaboration rights, and unblocking does not necessarily restore a prior collaboration without a fresh valid share or invitation.

Users may report Dressing Room users or messages in-app. K Scan AI may store the reporter, target user or content identifiers, room or message identifiers, report category, timestamps, status, and limited moderation context as necessary to investigate and enforce safety and policy requirements.

4.7 Shopping, Retailer, Marketplace, and Product Interaction Data

K Scan AI may process scan-derived product signals, search terms, item attributes, product identifiers, retailer or marketplace identifiers, product URLs, product images, saved items, and outbound-link interactions to return shopping options and retailer-neutral product results. Product availability, pricing, images, currency, and links may change or be incomplete.

When you open a third-party retailer or marketplace link, you leave K Scan AI and the third party's privacy policy applies. K Scan AI does not intentionally provide raw uploaded images to retailers for their independent use unless separately disclosed. K Scan AI may receive referral or affiliate compensation from qualifying outbound links, but the mobile apps do not use third-party advertising SDKs or Advertising ID for targeted advertising.

4.8 Approximate Location and Weather-Aware Styling

The mobile apps may request foreground location for optional weather-aware styling or localization. Depending on platform and operating-system settings, users may be able to choose the precision of location access. For weather-aware styling, K Scan AI uses approximate, rounded location context and does not store raw precise GPS coordinates for that feature. K Scan AI does not use background location for weather-aware styling. If you deny location access, core scanning, saving, Dressing Rooms, and Elise text functionality remain available, although weather-aware styling may be limited.

For weather-aware styling, the current implementation rounds latitude and longitude before the location context is supplied to the styling service. This produces an approximate area rather than sending raw precise GPS coordinates. K Scan AI does not store the raw precise coordinates for this feature. The Service may process the rounded location, request time, locale where available, and resulting local weather information as necessary to provide the requested styling context.

Approximate location may also be inferred from an IP address for security, localization, fraud prevention, or service delivery. K Scan AI does not use location for continuous tracking or to track users across third-party apps and websites for targeted advertising.

4.9 Device, App, Diagnostics, Security, and Elise Service Metadata

We may process device type, operating system, app version, package and build information, language settings, IP address, request metadata, authentication identifiers, app interactions, feature usage, error information, performance information, and security or fraud-prevention signals. The precise data depends on the feature used and the production configuration. K Scan AI does not use a third-party targeted-advertising SDK or collect Advertising ID.

To operate Elise and StyleChat, K Scan AI may also process account authorization, styling-session identifiers, message identifiers, timestamps, usage counts or quota information, model or provider information associated with generated replies, and references to scans, Closet items, Saved Looks, or Dressing Rooms that you intentionally use in the conversation. Authentication tokens, passwords, API keys, and raw device secrets are not intended to be part of Elise's fashion context.

4.10 Website, Cookies, and Similar Technologies

When you use the K Scan AI website, we may process browser, device, referral, traffic, cookie, and interaction data to operate the website, maintain security, measure performance, and understand usage. Where required by law, non-essential cookies or similar technologies are used only after valid consent.

5. How We Use Information

- Provide, operate, maintain, secure, and troubleshoot the Service.
- Authenticate users and maintain account, session, and actor isolation.
- Prepare selected images locally on supported upload flows, including re-encoding or metadata removal where available, before the requested remote analysis.
- Process single-image and multi-image scans and return fashion-related results.
- Provide Elise text responses, spoken responses, bounded recent conversation continuity, authorized fashion context, Signature Style personalization, and related AI functions.
- Use optional rounded approximate location and weather information to provide weather-aware styling when you enable that feature.
- Save and reopen Recent Scans and stored commerce snapshots.
- Operate Closet, Style Library, Saved Looks, owned Dressing Rooms, Shared with Me, room sharing, messages, and reactions.
- Return retailer-neutral shopping results and route users to third-party product pages.
- Prevent duplicate actions, abuse, fraud, unauthorized access, and cross-account data leakage.
- Enforce block relationships, investigate user or content reports and AI-response reports, moderate objectionable content, and apply safety or policy restrictions.
- Operate the account-deletion and restoration lifecycle, including deactivation, restoration, purge eligibility, verification, and related security or audit controls.

- Measure service reliability, diagnose errors, and improve product quality where permitted.
- Comply with law, respond to lawful requests, enforce terms, and protect users and the Service.
- Create aggregated or de-identified analytics and fashion or commerce insights for service improvement, planning, reporting, and other permitted business purposes.

6. AI Processing and Automated Results

K Scan AI uses cloud-hosted AI and automated systems to identify clothing and accessories, generate fashion attributes, match products, provide Elise responses, generate spoken audio, and personalize style assistance. Depending on the production configuration, providers may include Google Gemini, Supabase-hosted functions, ElevenLabs, and other authorized infrastructure or fallback providers.

K Scan AI's current fashion-context architecture is designed to provide AI systems with the fashion and conversation information needed for the requested feature rather than unrestricted access to all internal application data. Controlled fashion context may exclude local file paths, temporary image paths, authentication secrets, raw device identifiers, raw user identifiers, storage paths, signed storage URLs, internal detection coordinates, and other fields not needed for the styling task. The exact payload depends on the feature and current production implementation.

AI-generated results are probabilistic and may be incomplete, inaccurate, unavailable, offensive, or based on similar rather than exact products. K Scan AI does not guarantee product identity, brand, authenticity, price, currency, availability, fit, material, retailer listing, or recommendation accuracy. AI outputs are for fashion discovery and informational use, not professional, legal, medical, financial, authentication, or purchasing advice.

Elise is designed not to identify people or infer sensitive personal characteristics such as race, religion, health conditions, disability, sexual orientation, age, body measurements, or biometric identity from photographs, wardrobe information, account activity, name, or voice. However, users can voluntarily type sensitive information into free-text messages, and that text necessarily passes through the chat service before the Service can respond. Please avoid submitting sensitive information that is not needed for styling.

Users can report AI-generated responses from within K Scan AI without leaving the app. AI-response reports use structured reasons and limited allowlisted identifiers or context tied to the authenticated reporter. The report record is designed not to store the raw AI response, uploaded photos, scan media, or raw image content.

K Scan AI does not use AI to identify people, perform facial recognition, create biometric profiles, infer protected traits for legally significant decisions, or make decisions about employment, housing, credit, health care, insurance, or similar opportunities.

7. How We Disclose Information

K Scan AI may disclose information to service providers and other recipients only as reasonably necessary for the purposes described in this Policy, based on the feature used, user choices, app version, provider configuration, and legal requirements. We do not describe service-provider processing as zero retention, zero human review, or service-provider-only use unless the applicable production configuration and provider terms have been verified and separately disclosed.

8. Service Providers and Infrastructure

K Scan AI may use providers for authentication, database hosting, storage, cloud infrastructure, AI inference, text-to-speech, weather or localization support, product search, email, security, diagnostics, support, account deletion, and app operations. These providers may process account data, Submitted Visual Data, prompts, messages, fashion context, approximate location or weather context, generated audio, item metadata, diagnostics, and related information as necessary to provide their services.

K Scan AI uses reasonable contractual, technical, and organizational measures designed to have providers handle information consistently with this Policy and applicable law. Provider-specific logging, retention, safety review, quality improvement, deletion, and backup terms may apply. K Scan AI does not make a zero-retention, no-training, or no-human-review promise unless the applicable production configuration and provider terms have been verified and separately disclosed.

9. Retailer, Marketplace, and Product-Search Providers

K Scan AI may disclose limited fashion and product information, such as search terms, garment attributes, product signals, product identifiers, and product URLs, to product-search, commerce, affiliate, retailer, or marketplace providers to return relevant results and route users to third-party pages. K Scan AI does not claim an official retailer partnership merely because a retailer or marketplace appears in search or commerce results. When you visit a third party, its privacy policy and terms apply.

10. Analytics, Advertising, and Tracking Posture

K Scan AI may use first-party operational logs and basic usage information to maintain security, understand feature performance, diagnose errors, and improve the Service. The mobile apps do not use third-party advertising SDKs, do not collect Advertising ID for targeted advertising, and do not track users across third-party apps or websites for targeted advertising.

If K Scan AI later introduces cross-app tracking, targeted advertising, advertising SDKs, or activities requiring consent or App Tracking Transparency, K Scan AI will update this Policy and platform disclosures and request required consent before enabling those activities.

11. Sale, Sharing, Commercial Use, and De-identified Information

K Scan AI does not sell raw scans, uploaded images, Elise or StyleChat messages, private user-generated content, biometric identifiers, face templates, voiceprints, raw precise GPS coordinates, government identification, payment-card information, or sensitive personal information to third-party data buyers for independent use.

K Scan AI may use or disclose limited non-sensitive account, commerce, attribution, analytics, product-interaction, preference, or operational information where permitted by law and as described in this Policy. Depending on the data flow and applicable law, some disclosures to analytics, affiliate, commerce, or other partners may be considered a sale, sharing, targeted advertising, or similar regulated processing. Where required, K Scan AI will provide applicable notice, consent, or opt-out rights.

K Scan AI may create, use, disclose, license, or commercialize aggregated, anonymized, or de-identified fashion, product, commerce, and demand insights that do not reasonably identify a person, subject to controls designed to prevent re-identification. These insights may include trend, category, color, brand, product-interest, scan-volume, commerce, or market patterns at an appropriate level of aggregation.

12. Data Retention

K Scan AI retains information only as long as reasonably necessary for the purposes described in this Policy, unless a longer period is required or permitted by law. Retention depends on whether information is device-local, account-backed, transient for processing, part of a collaborative feature, needed for safety or security, or held by a service provider under applicable terms.

- Account and contact data: retained while the account is active and, after a deletion request is accepted, during the applicable restoration and deletion-processing lifecycle, subject to legal, security, fraud-prevention, dispute-resolution, and technical requirements.
- Device-local Recent Scans and device-local preference data: retained on the device until deleted in the app, app data is cleared, the applicable local feature removes it, or the app is uninstalled, subject to device and operating-system behavior. Cloud account deletion may not erase local data from an offline or disconnected device.
- Account-backed Closet, Style Library, Saved Look, and Dressing Room data: retained while the account is active or until the user deletes the applicable content or account, subject to shared-content, backup, security, fraud-prevention, and legal requirements. Content required to preserve an authorized continuing shared Dressing Room may be transferred, detached, or retained for remaining participants as described in Section 13.
- Submitted Visual Data used for AI processing: retained only as long as reasonably necessary to process the request, maintain security, troubleshoot, prevent abuse, comply with law, support requested history or saved content, or perform other purposes described in this Policy. Exact provider-side retention may depend on the applicable production configuration and provider terms.
- Prepared Images and temporary local image derivatives: may be retained temporarily on the device for the requested operation and removed through normal temporary-file or cache cleanup. K Scan AI does not promise that every image path uses identical temporary-file behavior.
- Elise and StyleChat messages: retained as needed to operate sessions, preserve requested conversation history, provide authorized styling context, troubleshoot, maintain security, and honor privacy requests. K Scan AI does not publish a fixed lifetime retention period for StyleChat messages unless one is separately established.
- Styling preferences and Signature Style data: device-local preferences or detailed feedback may remain on the device according to app-data lifecycle behavior; account-backed stylist preferences and derived fashion preference summaries may be retained while needed to personalize the account or until deleted or the account is purged, subject to legal and operational requirements.
- Approximate location and weather context: the current weather-aware styling feature does not store raw precise GPS coordinates. Rounded approximate location, request timing, locale, resulting weather information, or related operational records may be processed or retained only as reasonably necessary to provide the feature, maintain security, troubleshoot, or comply with law.

- Block relationships and UGC moderation reports: retained as safety or moderation records as reasonably necessary to enforce restrictions, investigate reports, prevent abuse, resolve disputes, and comply with law. Some records may survive account deletion with the deleted account reference removed or de-identified where necessary to preserve safety or audit integrity.
- AI-response reports: structured report metadata may be retained for moderation, safety, abuse prevention, policy enforcement, support, and audit purposes. The report record is designed not to store the raw AI-generated response, uploaded photos, scan media, or raw image content.
- Generated spoken-response audio: generally stored temporarily for playback and cache management rather than as a permanent user voice recording.
- Operational logs and diagnostics: retained for a reasonable period for security, reliability, troubleshooting, abuse prevention, and legal compliance. Provider or infrastructure logs may have separate retention cycles that are not determined solely by the mobile application source.
- Account-deletion lifecycle and audit records: K Scan AI may retain a limited de-identified or pseudonymous record of the deletion transaction, including status or processing information needed for security, compliance, auditing, and operational integrity, without retaining the normal active account relationship.
- Aggregated, anonymized, or de-identified information: may be retained for analytics, service improvement, planning, reporting, trend analysis, or permitted commercial insight uses if it cannot reasonably identify a person.

A valid deletion request does not erase all information immediately. When a deletion request is accepted, the account is deactivated and enters a limited restoration period of approximately 30 days. If the account is not restored and no legal, security, ownership, or technical hold applies, it becomes eligible for permanent deletion. Final purge may occur during a subsequent secure deletion cycle and is recorded as complete only after applicable verification checks. Residual copies may persist temporarily in access-controlled backups, logs, or provider systems under normal lifecycle processes or where retention is required or permitted by law. K Scan AI does not promise that every system or provider completes deletion at the exact moment the restoration period ends.

13. Account Deletion, Restoration, and Privacy Requests

You may request account deletion through the in-app Privacy or account settings where the deletion control is available, through the public deletion page, or by contacting K Scan AI. The external deletion resource is available at <https://kscan.app/legal/delete-account>. We may require authentication or additional verification before accepting or processing an account-specific request.

When K Scan AI accepts an account-deletion request, the account is deactivated and normal authenticated access is restricted. Existing sessions may be revoked or disabled. The deletion request enters a pending-deletion state and a restoration deadline is created. The account and account-linked information are intentionally retained during the restoration period so that an authorized restoration can be completed if the user changes their mind or the request was unauthorized.

K Scan AI currently provides a restoration period of approximately 30 days. Where available, K Scan AI may send a secure, limited-use restoration link to the account email address. Restoration links and tokens should be treated as sensitive credentials. A successful restoration cancels the pending deletion and requires a fresh sign-in; previously revoked sessions do not automatically become valid again.

If the account is not restored before the applicable deadline and no hold applies, the account becomes eligible for permanent deletion. Permanent deletion is a separate protected process from the Delete Account button. It is designed to remove the authentication account and account-linked personal information registered in the deletion process, including applicable profile data, account-backed scans and saved fashion content, Closet or wardrobe information, Style Library or inspiration items, Saved Looks, Elise or StyleChat conversations, styling preferences or memory, user-owned stored images, device-session records, and other user-bound application data.

Shared or collaborative content requires special handling. If a Dressing Room owned by the deleting user is actively shared with other authorized participants, K Scan AI may transfer the room to another eligible participant or retain content that is still required to preserve the continuing shared experience. Personal account references may be removed, detached, anonymized, or replaced with a neutral deleted-user reference where appropriate. Deleting your account does not require K Scan AI to delete another user's independent data or copies that another authorized user has already retained.

Some safety, moderation, fraud-prevention, dispute, legal, accounting, security, or audit records may be retained where reasonably necessary or permitted by law. K Scan AI may retain a minimized, de-identified, or pseudonymous deletion lifecycle record to demonstrate that a request was processed and to protect the integrity of the deletion system. Where required, K Scan AI may also revoke or remove authentication credentials associated with third-party sign-in providers when the corresponding K Scan AI account is permanently deleted.

K Scan AI does not treat a deletion as complete merely because deletion processing started or an authentication record was removed. The deletion lifecycle is intended to record a permanent purge as complete only after the deletion process completes applicable verification checks. Processing failures may be retried or require operational review rather than being silently treated as successful deletion.

Cloud account deletion does not necessarily remove device-local Recent Scans, caches, or other data stored solely on a device that is offline or no longer connected to the account. To remove local records, use available in-app deletion controls, clear app data, or uninstall the app. Deleting your K Scan AI account also does not automatically delete records independently controlled by app stores, retailers, marketplaces, payment processors, email providers, or other third parties.

Deletion may be delayed, paused, or limited where reasonably necessary to comply with law, respond to a legal or security hold, prevent fraud or abuse, resolve ownership disputes, protect the rights of other users, preserve required shared content, enforce agreements, maintain security, or address a technical failure. K Scan AI does not claim that deletion is immediate, complete across every third-party system, or fully automated in all circumstances.

14. Your Privacy Choices and Controls

- Use device settings to allow or deny camera, selected-photo, and approximate-location access.
- Choose whether to use optional weather-aware styling. Denying approximate location does not disable core scanning or Elise text functionality.
- Turn Elise Spoken Responses on or off where the app provides that control.
- Use available controls for Signature Style, feedback, stylist preferences, or optional styling context where those features are enabled.
- Delete individual Recent Scans, Closet or Style Library items, Saved Looks, Dressing Rooms, or memberships where the app provides those controls.
- Revoke room share links or remove Shared with Me memberships where available.
- Use available in-app controls to report objectionable Dressing Room users or messages, report AI-generated responses, and block users where supported.
- Request account deletion and, during an applicable restoration period, use the authorized restoration process if you change your mind.
- Request access, correction, deletion, export, restriction, objection, or withdrawal of consent where required by law.
- Opt out of marketing communications through the method included in the communication.
- Use any legally required sale, sharing, or targeted-advertising opt-out control if such processing is introduced or applicable.

Privacy requests may be submitted to kscanai.app@gmail.com. We may need to verify your identity before completing certain requests.

15. California and Other U.S. State Privacy Rights

Residents of California and other U.S. states with applicable privacy laws may have rights to know, access, correct, delete, obtain a copy of, or opt out of certain processing of personal information, and to avoid unlawful discrimination for exercising those rights, subject to legal exceptions. K Scan AI honors Global Privacy Control signals where required by law.

The mobile apps do not use third-party advertising SDKs or Advertising ID for targeted advertising. K Scan AI does not sell raw scans, uploaded images, Elise messages, private user-generated content, biometric data, raw precise GPS coordinates, or sensitive personal information to third-party data buyers for independent use. Some permitted analytics, commerce, attribution, or other disclosures may be considered sale or sharing under broad state-law definitions; where required, K Scan AI will provide applicable opt-out controls. Requests may be submitted through available in-app controls, <https://kscan.app/legal/delete-account>, or kscanai.app@gmail.com.

16. GDPR and UK GDPR Rights and Legal Bases

If you are located in the European Economic Area, United Kingdom, or another jurisdiction with similar rights, you may have rights to access, correct, delete, restrict, object, request portability, withdraw consent, and lodge a complaint with a supervisory authority.

Possible legal bases include performance of a contract for core Service delivery; consent where required for optional permissions, cookies, marketing, location, or other optional processing; legitimate interests for security, fraud prevention, diagnostics, service improvement, account support, abuse prevention, moderation, and commerce routing where lawful; and legal obligations. Where consent is required, withdrawal does not affect processing already completed lawfully before withdrawal.

17. International Data Transfers

Information may be processed in the United States and other countries depending on the providers and infrastructure used. Where required, K Scan AI uses lawful transfer mechanisms and safeguards, which may include Standard Contractual Clauses or other approved mechanisms. The mobile application source alone does not establish every provider's data-residency or subprocessor arrangement, and K Scan AI does not make an absolute residency claim unless separately verified and disclosed.

18. Security

K Scan AI implements reasonable administrative, technical, and organizational safeguards designed to protect information, including encryption in transit where appropriate, access controls, private storage where appropriate, actor-scoped authorization, data minimization, local image preparation on supported flows, and operational security practices. No system can be guaranteed completely secure, and K Scan AI does not use absolute-security, end-to-end-encryption, or zero-knowledge claims for the current mobile architecture unless separately verified and disclosed.

19. Children and Minor Safety

The Service is intended for adults 18 and older and is not directed to children or minors. If you believe a minor has provided information to K Scan AI, contact kscanai.app@gmail.com.

20. Third-Party Links and Retailer Transactions

The Service may link to third-party retailers, marketplaces, websites, or apps. K Scan AI is not responsible for third-party privacy practices, security, pricing, availability, authenticity, shipping, returns, payment processing, or customer service. Purchases are completed directly with the applicable third party unless K Scan AI expressly discloses otherwise.

21. Payments and Future Paid Features

Shopping actions route users to third-party pages for physical goods. K Scan AI does not process payment-card information for those purchases. If K Scan AI later offers paid digital features or subscriptions in the app, it will use Google Play Billing, Apple In-App Purchase, or other required payment methods and will update applicable disclosures.

22. Platform Privacy Disclosures

K Scan AI will maintain Google Play Data Safety, Apple App Privacy where applicable, and other platform disclosures that correspond to the applicable app build. Depending on the features used, reportable categories may include contact information, identifiers, photos and User Content, Elise or StyleChat messages, search terms, app activity, product interactions, styling preferences, diagnostics, approximate location, generated audio output, safety or moderation information, and pose/body-positioning context used for Mirror Selfie. Platform disclosures must be updated when permissions, SDKs, AI providers, storage practices, deletion practices, or data flows change.

23. Changes to This Policy

K Scan AI may update this Privacy Policy as the Service, data flows, providers, platform requirements, or law changes. For material changes, K Scan AI will provide additional notice or obtain consent where required. The Last Updated date will be revised when changes are published.

24. Contact Us

K Scan AI

Email: kscanai.app@gmail.com

Website: <https://kscan.app>

Full Privacy Policy: <https://kscan.app/legal/privacy>

Privacy Summary: <https://kscan.app/privacy>

Account Deletion: <https://kscan.app/legal/delete-account>

Appendix A - Current Data Category Summary

Category	Examples	Primary purpose
Contact information	Email address, name if provided, support communications	Authentication, support, notices, privacy requests
Identifiers	User ID, account ID, authentication/session identifiers, styling-session and message identifiers	Account security, actor isolation, conversation operation, diagnostics

Photos and User Content	Selected images, prepared image derivatives, scans, Elise/StyleChat messages, room content, inspiration uploads	Scanning, AI styling, saving, sharing, support
Fashion and styling preferences	Helpful / Not My Style feedback, optional styling context, commonly selected brands/categories/colors, general price-range signals	Personalize Elise and fashion recommendations
Search and commerce data	Product queries, item attributes, retailer links, saved commerce snapshots	Product matching, retailer-neutral routing, reopen behavior
App activity	Feature usage, save actions, room actions, outbound-link interactions	App functionality, reliability, fraud prevention, internal analytics
Approximate location	Optional rounded foreground location for weather styling; IP-derived region where applicable	Optional weather context, localization, security
Diagnostics	Error, performance, request, operational, and security logs	Troubleshooting, reliability, security
Audio output	Generated Elise speech audio and timing data	Text-to-speech playback; no microphone recording
Financial information	Payment-card data for retailer purchases	Not collected by K Scan AI in the current third-party checkout flow
Sensitive information	Not intentionally requested; may appear incidentally in images or free-text messages	Users should avoid submitting sensitive or non-fashion information
Safety and moderation	Block relationships, UGC reports, AI-response report metadata and allowlisted identifiers/context	User safety, abuse prevention, moderation, policy enforcement, support
Pose/body-positioning context	User-requested Mirror Selfie image/pose signals where used	Fashion visualization; not facial recognition or biometric identification
Deletion lifecycle data	Deletion status, request/restoration timing, limited verification/audit information, pseudonymous or de-identified deletion record	Account deletion, restoration, security, compliance, operational integrity
Aggregated or de-identified insights	Fashion, product, commerce, demand, trend, or usage patterns that do not reasonably identify a person	Analytics, planning, reporting, service improvement, permitted commercial insights