

Glimpse — Guest Face-Match Consent & Privacy Controls

Product Requirements Document · Sample · Aryan Shirke

This is a sample PRD, written to show how I structure product requirements — not an excerpt from an actual release. The product (Glimpse) and its underlying face-matching engine are real; the feature, metrics, and rollout below are illustrative.

1. Overview

Glimpse's core value prop is AI face-clustering: guests find every photo they're in without scrolling through an event's full shared album. Today, matching runs by default for every guest who opens an event gallery — there is no explicit opt-in, and no guest-facing way to see or delete face data afterward. As Glimpse moves toward corporate and multi-day event customers, we need an explicit consent and control layer around face-matching, without adding enough friction that guests abandon the “find my photos” flow that makes the product worth using.

2. Problem

- Guests are matched by default; several corporate organizers have asked whether attendees can opt out.
- There is no user-facing way to see what face data Glimpse holds, or to request deletion.
- Support has fielded a handful of “how do I remove myself” requests that currently require manual backend intervention.

3. Goals

- Give guests explicit, low-friction control over face-matching, without materially hurting match-flow completion.
- Give organizers a data-handling story to tell privacy-conscious attendees.
- Make guest-initiated deletion fully self-serve.

4. Non-goals

- Not building a general-purpose consent-management platform.
- Not changing the underlying VirAI clustering model or its match accuracy.
- Not supporting granular per-photo consent — all-or-nothing per event for v1.

5. User stories

- As a guest, I want to know before my face is matched, so I can decide whether to participate.

- As a guest, I want to delete my face data after an event, so it is not retained indefinitely.
- As an organizer, I want to tell attendees Glimpse handles face data responsibly, so I can get buy-in from privacy-conscious guests and companies.

6. Requirements

Functional

- On first visit to an event gallery, show a one-time, dismissible consent prompt ("Let us find your photos automatically?") with Yes / No.
- Guests who decline can still browse and search manually; guests who accept get the automatic face-matched view.
- A "Remove my face data" flow is reachable from the guest's matched-photos view and from any transactional email, and requires only email confirmation — no account needed.
- Deletion removes the guest's face embedding and matched-photo associations within 24 hours; it does not delete the original event photos.

Technical

- Consent state is stored per (event_id, guest_session) pair, not tied to a persistent user profile — most Glimpse guests are unauthenticated.
- Face embeddings for opted-out or deleted guests are purged from the clustering index, not just hidden in the UI.
- Deletion requests are logged for an organizer-facing audit trail (count only — no guest PII exposed to the organizer).

7. Success metrics

- Consent opt-in rate $\geq 80\%$ — the bar for "does not materially hurt the core flow."
- $< 2\%$ increase in time-to-first-match after adding the prompt.
- Deletion requests fulfilled within the 24-hour SLA $\geq 99\%$ of the time.
- At least one corporate customer cites the consent flow as a reason they signed or renewed (qualitative).

8. Rollout

Ship behind a flag to 2–3 existing corporate-event organizers first, and compare opt-in rate and support-ticket volume against the current default-on baseline. If opt-in holds $\geq 80\%$ with no meaningful support regression, roll out to all new events; events already in flight keep default-on matching with a banner offering opt-out.

9. Open questions

- Should guests who opt out still be able to see which of their photos exist via manual browse, or is that itself a privacy question worth separating out?

- Does a guest's consent choice need to persist across multiple events, or should it reset each time?