ProjectX

VERIFY · DATASHEET

Customer verification with consent, review and evidence.

Identity verification as a guided journey: applicants, consent capture, provider-neutral checks and dual-controlled review, with an evidence trail you can put in front of an auditor.

Why teams choose it

01
Consent before every check
No check runs without recorded consent, captured as part of the journey — so your compliance storey starts at the first click, not at the audit.

02
Documents stay in their region
Identity documents never leave the region they belong to. The platform holds references, not the documents themselves — your data-residency posture is structural, not promised.

03
Decisions you can explain
Every outcome carries its reason codes, resubmission is an explicit step, and sensitive decisions need a second, independent reviewer — no unexplained rejections.

04
Deletion you can prove
Retention limits are enforced by the platform, and deletion produces verifiable evidence — a stable record that the data was removed.

In numbers

2
matching reviewers for a business or high-risk case

0
credits for an abandoned or platform-failed attempt

1 year
at most, for a reusable identity before it expires

What it does

Applicants and versioned flows

Each applicant moves through a versioned flow of ordered checks. Every attempt is recorded immutably, and sensitive documents never sit in the platform's core records.

The flow is versioned, so every applicant gets the same journey and a change to the journey is itself a tracked event. Every attempt is recorded immutably, and sensitive documents stay out of the platform's core records.

Consent and regional residency

No check runs without recorded consent, and identity documents stay inside the region they belong to — the platform holds references, not the documents themselves.

Consent is captured as a step of the journey itself, before anything runs. Documents stay in the region they belong to and the platform keeps references — so your data-residency posture is structural, not promised.

Explainable outcomes and dual control

Every outcome carries its reason codes, resubmission is an explicit step, and sensitive decisions require a second, independent reviewer.

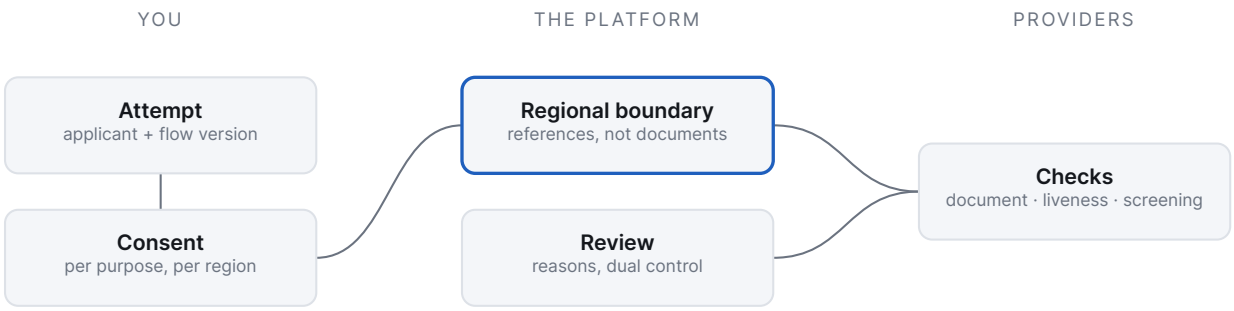
A rejection comes with its reason codes and an explicit resubmission step, so an applicant is never turned away unexplained. The decisions you cannot afford to get wrong need a second, independent reviewer before they stand.

Retention and deletion evidence

Retention limits are enforced, and deletion produces verifiable evidence — a stable record that the data was removed, with premature deletion refused.

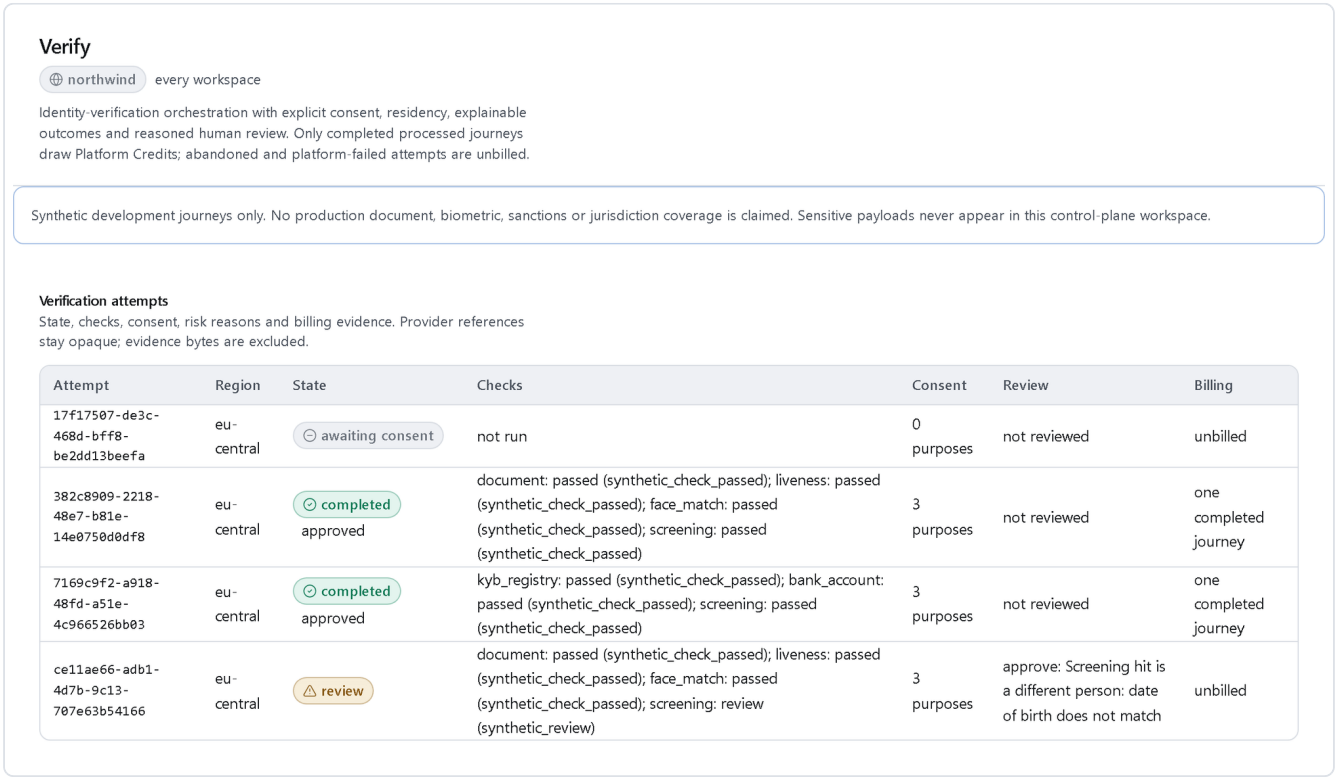
Set the retention limit and the platform enforces it. When the time comes, deletion produces verifiable evidence — a stable record that the data was removed — and a deletion attempted early is refused.

How it fits together



An attempt binds one applicant to one flow version. Consent comes first and is checked against the applicant's region. The checks go to a provider behind a regional boundary, and a case that needs a person goes to review, where sensitive decisions need two.

In the console



Verify

northwind every workspace

Identity-verification orchestration with explicit consent, residency, explainable outcomes and reasoned human review. Only completed processed journeys draw Platform Credits; abandoned and platform-failed attempts are unbilled.

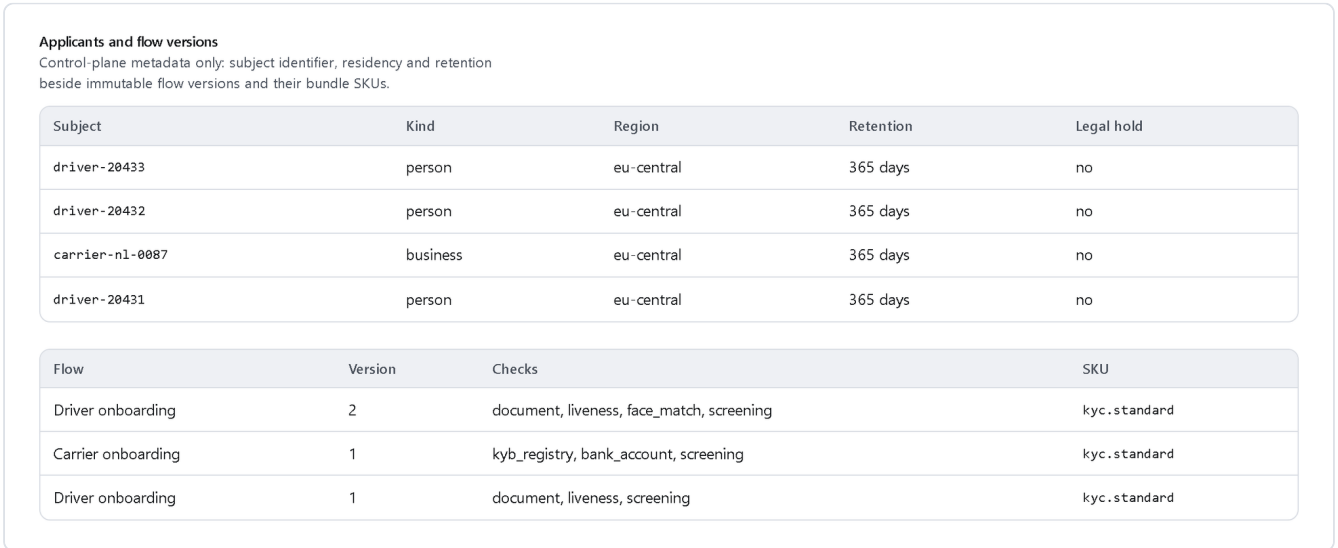
Synthetic development journeys only. No production document, biometric, sanctions or jurisdiction coverage is claimed. Sensitive payloads never appear in this control-plane workspace.

Verification attempts

State, checks, consent, risk reasons and billing evidence. Provider references stay opaque; evidence bytes are excluded.

Attempt	Region	State	Checks	Consent	Review	Billing
17f17507-de3c-468d-bff8-be2dd13beefa	eu-central	awaiting consent	not run	0 purposes	not reviewed	unbilled
382c8909-2218-48e7-b81e-14e0750d0df8	eu-central	completed approved	document: passed (synthetic_check_passed); liveness: passed (synthetic_check_passed); face_match: passed (synthetic_check_passed); screening: passed (synthetic_check_passed)	3 purposes	not reviewed	one completed journey
7169c9f2-a918-48fd-a51e-4c966526bb03	eu-central	completed approved	kyb_registry: passed (synthetic_check_passed); bank_account: passed (synthetic_check_passed); screening: passed (synthetic_check_passed)	3 purposes	not reviewed	one completed journey
ce11ae66-adb1-4d7b-9c13-707e63b54166	eu-central	review	document: passed (synthetic_check_passed); liveness: passed (synthetic_check_passed); face_match: passed (synthetic_check_passed); screening: review (synthetic_review)	3 purposes	approve: Screening hit is a different person: date of birth does not match	unbilled

Each attempt with its checks, consent, review and whether it was billed. Screens shown with demo data.



Applicants and flow versions

Control-plane metadata only: subject identifier, residency and retention beside immutable flow versions and their bundle SKUs.

Subject	Kind	Region	Retention	Legal hold
driver-20433	person	eu-central	365 days	no
driver-20432	person	eu-central	365 days	no
carrier-nl-0087	business	eu-central	365 days	no
driver-20431	person	eu-central	365 days	no

Flow	Version	Checks	SKU
Driver onboarding	2	document, liveness, face_match, screening	kyc.standard
Carrier onboarding	1	kyb_registry, bank_account, screening	kyc.standard
Driver onboarding	1	document, liveness, screening	kyc.standard

Applicants hold references, not documents; flows are versioned. Screens shown with demo data.

Key ideas

Flow version
The ordered checks an applicant goes through and the SKU it bills. A new version is a new flow; an attempt keeps the version it started on.

Payload boundary
Documents and images stay in the applicant's region. The platform keeps a reference, and nothing goes to a provider without consent for that purpose in that region.

Reusable identity
An approved verification that a later attempt can rely on without calling the provider again, until it expires or is revoked. It bills at its own reuse rate.

In depth

Billing only for an answer
A completed attempt bills once, whatever is retried. An attempt the applicant abandons, or one that failed because a provider was down, is never billed.

Businesses, not only people
Company registry and bank-account checks are steps in the same flows, behind the same consent rules, and a business subject always needs two reviewers.

After onboarding
Standing subscriptions re-screen an applicant at most daily against watchlists, fraud signals and transactions. A non-passing result opens one alert, and only a named reviewer with a written reason can close it.

Regulated reporting
Reporting profiles state the jurisdiction, regulator and threshold. Transfers at or above it go through the Travel Rule provider before they are acknowledged, and filing a report is a named act.

How it works

01 **Define your journey** · Console
Versioned flows order the checks an applicant goes through, so every applicant gets the same journey.

02 **Capture consent, then check** · API
No check runs without recorded consent; documents stay in their region while the platform keeps references.

03 **Review the edge cases** · Console
Outcomes carry reason codes, and sensitive decisions get a second, independent reviewer.

04 **Keep the evidence** · Audit trail
Retention is enforced, and deletion produces verifiable evidence you can put in front of an auditor.

Who it is for

Fintech and payments

You must verify customers before they move money, with evidence for regulators.

Guided journeys with consent capture, explainable outcomes and an audit-ready trail.

Marketplaces

Sellers and buyers must be who they say they are, at scale.

Versioned flows that give every applicant the same journey and every decision a reason code.

Restricted services

Access depends on identity or age checks you cannot get wrong.

Dual-controlled review for sensitive decisions and residency rules the platform enforces.

Works with

Console · API · Audit trail

Questions buyers ask

What does the applicant see?
A guided journey: the versioned flow orders the checks, consent is captured before anything runs, and a rejection comes with reason codes and an explicit resubmission step.

Where do identity documents go?
They stay inside the region they belong to. The platform’s core records hold references, not the documents, so residency is enforced structurally.

Who reviews the edge cases?
Sensitive decisions require a second, independent reviewer — dual control is built into the review step, not bolted on.

How long is verification data kept?
Only as long as the retention limit you set. Deletion then produces verifiable evidence, and premature deletion is refused.

How is it priced?
Per verification at published usage rates in Platform Credits, on the same invoice as the rest of the platform. The rates are on the pricing page.

Pricing

Current published rates, in your currency: https://adaydev.com/pricing/products/verify