Veyns Biometric Policy

Effective date: October 17, 2026

1. ABOUT THIS POLICY

Veyns provides palm-vein biometric authentication infrastructure to banks, payment service providers (PSPs), and identity application providers ("partners"). This policy explains, in plain language, what biometric information is involved when you enroll or authenticate with your palm at a Veyns-enabled terminal or application, how it is protected, who can access it, and how you can have it deleted.

2. WHAT WE COLLECT

When you enroll, a contactless near-infrared palm scanner reads the vein pattern of each hand (left and right). The capture software converts this pattern into a mathematical representation — a biometric template and matching features.

We collect and process only:

- Biometric templates and features derived from your palm-vein pattern
- Technical metadata required to operate the service (terminal identifier, timestamps, authentication outcomes)

We do not collect facial images, fingerprints, voice recordings, or any other biometric modality.

3. YOUR PALM IMAGES NEVER LEAVE THE DEVICE

Raw palm images are processed in the capture device's memory only and are permanently discarded the moment the biometric template is extracted. They are never saved to storage and never transmitted over any network. Veyns systems are architected so that no raw palm image exists beyond the capture device. The live preview shown during capture is privacy-masked.

4. WHAT OUR SERVERS HOLD

Our palm service holds:

- Your biometric templates, encrypted at rest using AES-256-GCM
- An opaque system identifier — not your name or contact details associated with those templates
- Security and audit logs of authentication events (time, terminal, outcome)

Your name, phone number, and any other enrollment details you provide to your bank or payment provider remain with that partner and are not transmitted to Veyns.

5. HOW YOUR BIOMETRIC DATA IS USED

Your biometric data is used for one purpose only: to verify that the person presenting a palm is the enrolled person, for a payment or sign-in that you initiated. Matching is performed within our protected palm service, which returns a match result only.

We do not use biometric data for profiling, analytics, advertising, or any purpose other than authentication.

6. WHO RECEIVES YOUR BIOMETRIC DATA

No partner, merchant, or third party ever receives your biometric templates, features, images, or match scores.

- Banks and PSPs receive a digitally signed (Ed25519) authentication confirmation bound to the specific transaction, together with a pseudonymous identifier that is unique to that partner and cannot be correlated across organizations.
- Biometric matching software runs entirely within Veyns-controlled infrastructure. No biometric data is sent to any vendor cloud or external matching service.
- Biometric data is never sold, rented, or shared for marketing.

7. LIVENESS AND ANTI-SPOOFING

Every Veyns capture device performs liveness and presentation-attack detection built on the ISO/IEC 30107-3 framework, designed to reject photographs, recordings, replicas, and other artifacts. A failed liveness check ends the authentication attempt immediately. Our biometric accuracy evaluation programme follows the ISO/IEC 19795-1 testing methodology.

8. RETENTION AND DELETION

Your biometric templates are retained only while your enrollment remains active. Templates are permanently deleted from the matching index and all operational databases when:

- you withdraw your consent,
- you close the linked account with your participating partner, or
- your partner instructs us to delete the enrollment.

Security and audit logs relating to authentication events are retained for limited periods required for fraud prevention and dispute handling, then deleted or anonymized.

9. HOW WE PROTECT BIOMETRIC DATA

- Encryption in transit (TLS) and at rest (AES-256-GCM)
- Device keys held in hardware-backed keystores (Android StrongBox / Trusted Execution Environment) where available.
- Every terminal individually identified and cryptographically signing its requests.
- Administrative access restricted, authenticated, and audited.
- Templates stored under opaque identifiers, separated from personal details.

10. CONSENT AND YOUR RIGHTS

Enrollment is voluntary and based on your explicit consent, collected by the participating bank, PSP, or identity provider (the data controller) at enrollment time. Veyns processes biometric data solely on that partner's documented instructions, as a data processor. You may withdraw consent or request access to, correction of, or deletion of your biometric data at any time through your participating partner. You may also contact us directly at info@veyns.io and we will route your request to the appropriate organization.

11. LIMITATION OF LIABILITY

Veyns provides biometric authentication technology designed to facilitate identity verification through the transient processing of mathematical representations derived from palm-vein characteristics.

Veyns does not operate a centralized biometric database and does not retain biometric images or biometric templates within its infrastructure as part of its stated authentication architecture. Biometric representations are processed transiently for authentication purposes, subject to the technical configuration and operating arrangements of the relevant service.

Veyns acts as a technology enabler and shall not automatically be deemed responsible for the independent collection, enrollment, retention, management or use of biometric information by third-party organizations integrating its technology. The respective responsibilities of Veyns and each integrating organization shall be determined by their actual processing activities, contractual arrangements and applicable law.

To the fullest extent permitted by law, Veyns shall not be liable for losses arising exclusively from unauthorized modifications, improper integrations, third-party security failures, misuse of authentication credentials or actions beyond its reasonable control, except where attributable to Veyns' own acts, omissions or legal obligations.

Veyns does not warrant that biometric authentication technology is infallible, immune to presentation attacks, or capable of preventing every instance of identity fraud, unauthorized access or security compromise.

Nothing in this Policy shall exclude, restrict or diminish any mandatory legal responsibility of Veyns, including obligations relating to data protection, information security, fraud, gross negligence or wilful misconduct.

12. CHANGES TO THIS POLICY

We may update this policy from time to time. The current version, with its effective date, is always available at https://veyns.io/biometric-policy. Material changes will be communicated through our partners before they take effect.

13. CONTACT

Email: info@veyns.io
Website: https://veyns.io

Privacy Policy: https://veyns.io/privacy