Veyns Privacy Policy

1. WHO WE ARE

Veyns provides biometric identity verification and payment authentication infrastructure, including palm-vein matching services, managed payment terminals, and the Veyns ID identity platform, to banks, payment service providers (PSPs), and application developers (collectively referred to as “Partners”).

This Privacy Policy explains how Veyns collects, processes, uses, protects, retains, and discloses personal information in connection with its services, technology infrastructure, identity platform, and website.

Information relating specifically to the processing of biometric data is addressed in our separate Biometric Policy, available at:

https://veyns.io/biometric-policy

This Privacy Policy should be read in conjunction with the Biometric Policy where biometric authentication services are involved.

2. OUR ROLE IN DATA PROCESSING

Veyns processes personal information in different capacities depending on the nature of the service and its relationship with the individuals or organizations concerned.

2.1. End User Information

Where individuals enroll in or use Veyns enabled services through a bank, payment service provider, identity provider, or other Partner institution, that Partner acts as the data controller. Veyns acts as a data processor and processes end user personal information, including biometric information, solely in accordance with the documented instructions of the relevant Partner.

The Partner remains responsible for determining the purposes and means of processing personal information relating to its end users.

2.2. Partner Business Contacts

Veyns acts as the data controller in respect of personal information collected and processed in connection with its direct business relationships with Partner organizations, including information relating to their representatives and business contacts.

2.3. Website Visitors

Veyns acts as the data controller for personal information collected directly through the operation and administration of its website.

3. INFORMATION WE PROCESS

The categories of personal information processed by Veyns depend on the services provided, the nature of the relevant relationship, and the technical requirements of each deployment.

3.1. End-User Information Processed on Behalf of Partners

In providing biometric authentication and payment-related services on behalf of Partners, Veyns may process the following information:

a. Biometric Information

Encrypted palm-vein biometric templates and associated biometric features used to facilitate identity verification and authentication.
Raw palm-vein images are discarded locally on the capture device and are not transmitted to or stored on Veyns servers.
Further information concerning the handling, processing, and protection of biometric information is provided in the Veyns Biometric Policy.

b. Transaction Information

Transaction metadata necessary to associate an authentication event with a specific payment or commercial transaction, including:

- Transaction amount;
- Transaction currency; and
- Merchant reference identifiers.

Veyns does not receive or store payment card numbers.

c. Device and Security Information

Technical and operational information necessary to facilitate authentication, maintain system integrity, and support security monitoring, including:

- Terminal and device identifiers;
- Authentication results and outcomes;
- Security and operational logs; and
- Internet Protocol (IP) addresses.

3.2. Veyns ID Account Information

Where an individual uses the Veyns ID identity platform, Veyns may process the following account-related information:

- Account identifiers;
- Information relating to paired devices and their assigned labels;
- Public cryptographic keys;
- Cryptographic hashes of recovery codes; and
- Remembered scanner associations.

Remembered scanner associations are maintained for a period of up to thirty (30) days.

3.3. Partner Organization Information

In connection with the provision, administration, and technical support of its services to Partner organizations, Veyns may process:

a. Business Contact Information

- Names of authorized representatives and business contacts;
- Business email addresses; and
- Business telephone numbers.

b. API Authentication Information

Application programming interface (API) credentials, which are stored exclusively in cryptographically hashed form.

c. Managed Device Information

Operational telemetry relating to managed terminal and device fleets, including:

- Device models;
- Battery status;
- Network connectivity and status; and

- Installed software versions.

3.4. Website Information
When individuals access the Veyns website, standard web server logs may be generated and processed for operational and security purposes.
Such information may include:
- IP addresses;
- Browser types; and
- Pages requested or accessed.

Veyns does not use third-party advertising trackers or third-party analytics trackers on its website.

4. INFORMATION WE DO NOT COLLECT
Veyns limits its processing of personal information to the categories necessary for the operation and delivery of its services.
Veyns does not collect or retain the following categories of information:
4.1. Raw Palm Images
Raw palm images captured during biometric enrollment or authentication are discarded on the capture device and are not transmitted to Veyns servers.
4.2. Precise Location Information
Veyns does not collect precise geographical location data.
4.3. Personal Device and Advertising Information
Veyns does not collect contact lists, browsing histories, or advertising identifiers.
4.4. Payment Card Information
Veyns does not collect, receive, or store payment card numbers.

5. PURPOSES OF PROCESSING
Veyns processes personal information only for purposes connected with the provision, operation, administration, and security of its services.
These purposes include:
5.1. Authentication and Identity Services
Providing biometric authentication, identity verification, and associated identity services through Veyns-enabled infrastructure and applications.
5.2. System Operations and Security
Operating, maintaining, securing, monitoring, and auditing Veyns systems, services, devices, and supporting infrastructure.
5.3. Fraud Prevention
Detecting, preventing, and responding to fraudulent activity, including attempted biometric presentation attacks and other authentication-related security threats.
5.4. Contractual Service Delivery
Providing operational, technical, and administrative support to Partners in accordance with the applicable contractual arrangements.
Veyns does not sell personal information to third parties.
Veyns does not process personal information for advertising purposes.

6. SHARING AND DISCLOSURE OF INFORMATION

Veyns restricts the disclosure of personal information to circumstances necessary for the delivery of its services, the operation of its infrastructure, or compliance with applicable legal requirements.

6.1. Partner Organizations

Veyns provides Partners with digitally signed authentication results accompanied by pseudonymous identifiers.

Biometric information is not disclosed to Partners as part of these authentication results.

6.2. Infrastructure Hosting Providers

Infrastructure hosting providers may process information in connection with the hosting and operation of Veyns services.

Such processing takes place within Veyns' secured operating environment and remains subject to Veyns' control and instructions.

6.3. Legal and Regulatory Disclosure

Veyns may disclose personal information to competent authorities where such disclosure is required under applicable law.

Veyns does not disclose personal information to authorities except where legally required to do so.

7. DATA RETENTION AND DELETION

Veyns retains personal information only for the periods applicable to the relevant service, processing purpose, or contractual relationship.

Retention arrangements differ according to the category of information concerned.

7.1. Biometric Information

Biometric templates are retained only for as long as the relevant biometric enrollment remains active.

Upon withdrawal of consent or receipt of an applicable instruction from the relevant Partner, the associated biometric templates are permanently deleted in accordance with the Veyns Biometric Policy.

7.2. Transaction Records and Security Logs

Transaction journals and security logs are retained for limited periods consistent with applicable fraud prevention, dispute resolution, and audit requirements.

Following the applicable retention period, such records are deleted or anonymized.

7.3. Partner Account Information

Information associated with Partner accounts and business relationships is retained for the duration of the relevant business relationship and for any additional period required under applicable law.

7.4. Remembered Scanner Associations

Remembered scanner associations associated with Veyns ID are maintained for a maximum period of thirty (30) days.

8. INFORMATION SECURITY

Veyns implements technical and organizational security measures designed to protect personal information against unauthorized access, disclosure, alteration, and misuse.
These measures include:

8.1. Encryption

Encryption of personal information during transmission and while stored within Veyns infrastructure.

8.2. Hardware-Backed Device Security

The use of hardware-backed cryptographic device keys to support secure device identification and authentication.

8.3. Cryptographic Request Authentication

Per-terminal cryptographic request signing to support the authenticity and integrity of communications originating from managed terminals.

8.4. Access Restrictions

Deny-by-default access controls governing access to services and infrastructure.

8.5. Administrative Access Controls

Authenticated and audited administrative access to systems and infrastructure.
These safeguards form part of Veyns' approach to maintaining the confidentiality, integrity, and security of information processed through its services.

9. INTERNATIONAL OPERATIONS AND DATA RESIDENCY

Veyns operates internationally, with its primary operations located in the United Arab Emirates. Depending on the nature and jurisdiction of a particular deployment, the processing of personal information may be governed by applicable data protection legislation, including:

- **United Arab Emirates:** Federal Decree-Law No. 45 of 2021 Regarding the Protection of Personal Data.
- **British Virgin Islands:** Data Protection Act, 2021.

The data residency requirements and commitments applicable to a particular Partner deployment are established in the relevant deployment agreement.
The applicable contractual arrangements determine the data residency commitments governing the processing and hosting of information associated with that deployment.

10. YOUR PRIVACY RIGHTS

Depending on the data protection legislation applicable to an individual and the circumstances of the relevant processing activity, individuals may have certain rights in relation to their personal information.
These rights may include:

10.1. Right of Access

The right to request access to personal information held or processed in relation to the individual.

10.2. Right to Rectification
The right to request the correction of inaccurate or incomplete personal information.
10.3. Right to Erasure
The right to request the deletion of personal information, subject to applicable legal requirements.
10.4. Withdrawal of Consent
The right to withdraw consent where consent forms the basis for the relevant processing activity.
10.5. Right to Object
The right to object to certain processing activities where such a right is provided under applicable law.
10.6. Right to Lodge a Complaint
The right to submit a complaint to the relevant supervisory or regulatory authority, where permitted under applicable law.

Exercising Your Rights
Where personal information is processed through a Partner institution, individuals should direct requests concerning their personal information to the institution through which they enrolled or accessed the relevant service.
This may include their bank, payment service provider, or identity provider.
Individuals may also contact Veyns at **info@veyns.io**.
Where a request concerns information processed by Veyns on behalf of a Partner, Veyns will direct the request to the appropriate organization.

11. CHILDREN'S PRIVACY
Veyns services are provided to adults through Partner institutions and are not intended for or directed toward children.
Veyns does not knowingly collect personal information from children.

12. LIMITATION OF LIABILITY
Veyns operates as a technology infrastructure provider, enabling identity verification, authentication and related services through its technology, software, hardware and integrations.
To the fullest extent permitted by applicable law, Veyns shall not be liable for any indirect, incidental, consequential, special or punitive damages, including loss of profits, business opportunities, revenue or data, arising from the use of, inability to use or reliance upon its services.
Veyns shall not be responsible for the independent acts, omissions, security practices, data processing activities or regulatory obligations of third-party institutions, merchants, financial service providers, developers or integration partners utilizing its technology, except to the extent such liability is directly attributable to Veyns or otherwise imposed by applicable law.
Each participating organization remains responsible for its independent collection, use, storage, disclosure and protection of personal information, including compliance with applicable privacy, consumer protection and data protection legislation.

While Veyns implements reasonable technical and organizational safeguards appropriate to its operations, no technology infrastructure can be guaranteed to be entirely free from vulnerabilities, disruptions or unauthorized interference.
Nothing in this Policy shall exclude or restrict liability arising from fraud, gross negligence, wilful misconduct, violations of mandatory data protection obligations or any other liability that cannot lawfully be excluded or limited.

13. CHANGES TO THIS PRIVACY POLICY

Veyns may amend or update this Privacy Policy from time to time to reflect changes in its services, operational practices, or applicable requirements.
The current version of this Privacy Policy, together with its effective date, will be made available at: https://veyns.io/privacy
Where changes to this Privacy Policy are material, Veyns will communicate such changes through its Partners before they take effect.

14. CONTACT INFORMATION

For inquiries concerning this Privacy Policy, the processing of personal information, or the exercise of applicable privacy rights, individuals and Partner organizations may contact Veyns using the following details:
Veyns
Email: info@veyns.io
Website: https://veyns.io
Privacy Policy: https://veyns.io/privacy
Biometric Policy: https://veyns.io/biometric-policy