

OPULUME INFORMATION SECURITY STATEMENT

EffectiveDate: June 30th, 2026

Last Updated: June 30th, 2026

1. Our Commitment

Opulume is committed to protecting the confidentiality, integrity and availability of the personal information entrusted to us. We implement technical, organisational and administrative safeguards designed to protect user information against unauthorised access, disclosure, alteration, loss and misuse.

Our security programme is based upon recognised information security principles including data minimisation, least-privilege access, defence in depth, secure authentication and continuous monitoring.

2. Authentication & Identity Security

Opulume protects user accounts through multiple authentication controls, including:

- Secure email and password authentication;
- Google Sign-In;
- Apple Sign-In;
- bcrypt password hashing with appropriate salt rounds;
- JSON Web Token (JWT) authentication;
- JWT versioning to invalidate compromised sessions;
- Secure HTTP-only cookies where applicable;
- SameSite=Strict cookie protection;
- HTTPS-only secure cookie transmission;
- Authentication rate limiting;
- One-time verification codes with automatic expiry.

Passwords are never stored in plaintext.

3. Encryption

Information is protected using encryption both in transit and, where supported by our infrastructure providers, at rest.

Security measures include:

- TLS/SSL encrypted communications;
- encrypted hosting infrastructure;
- encrypted databases and cache storage where supported;
- signed authentication tokens;
- secure transmission protocols.

4. Access Controls

Access to personal information is restricted according to the principle of least privilege.

Current access roles include:

- User access to their own information only;
- Limited administrative access for operational functions;
- No routine administrator access to individual wellness information;
- User-controlled practitioner sharing where implemented.

Access permissions are regularly reviewed.

5. Health Information Protection

Health and wellness information is treated as sensitive personal information.

Access is limited to authorised processing necessary to provide the Service and is subject to explicit user consent where required by applicable data protection legislation.

6. Skin Image Processing

Skin photographs submitted for analysis are subject to a data minimisation approach.

Images are:

- processed transiently;
- analysed in memory;
- permanently discarded immediately after processing;
- never retained in production databases;
- never maintained as image libraries.

Only the resulting analysis may be retained in accordance with the applicable retention policy.

7. Infrastructure Security

Opulume utilises professionally managed cloud infrastructure with security features that may include:

- firewalls;
- encrypted storage;
- network isolation;

- automated backups;
- infrastructure monitoring;
- security patch management.

Infrastructure providers are selected following appropriate due diligence.

8. Monitoring & Logging

Security monitoring supports detection of:

- authentication failures;
- suspicious login activity;
- abuse;
- excessive request rates;
- operational anomalies.

Operational logs are retained only as necessary and anonymised in accordance with our retention policies.

9. Incident Response

Opulume maintains procedures for responding to suspected security incidents.

Where appropriate these may include:

- investigation;
- containment;
- credential invalidation;
- recovery;
- user notification;
- regulatory notification where legally required.

Where a personal data breach is likely to result in a risk to individuals, notifications will be made in accordance with applicable law.

10. Third-Party Processors

We carefully select third-party service providers that support secure operation of the Service.

Processors are expected to maintain appropriate technical and organisational security measures and contractual safeguards.

11. User Responsibilities

Users also play an important role in protecting their accounts.

Users should:

- maintain secure passwords;
 - protect their devices;
 - keep authentication credentials confidential;
 - report suspected unauthorised access promptly;
 - install application updates.
-

12. Continuous Improvement

Information security is an ongoing process.

We periodically review and improve our security controls in response to:

- evolving threats;
 - technological developments;
 - legal requirements;
 - operational experience;
 - industry best practice.
-

13. Contact

Questions regarding information security may be directed to:

Opulume Limited

Email: customerservice@opulumeskin.com

Website: www.opulumeskin.com