Privacy Notice - Sylton Connect

Version: Jan 13th, 2026

This Privacy Notice is issued by InnoFaith Beauty Sciences B.V. and its affiliated entity, Sylton International B.V. (hereinafter referred to as “InnoFaith,” “Sylton International,“ “we,” “us,” or “our”).

Our Products and Services may carry the InnoFaith or Sylton brand name.

This privacy notice applies to Sylton Connect, a product marketed by Sylton International and provided by InnoFaith.

This Privacy Notice explains how we collect, use, and safeguard personal data from you and your patients when using the Sylton Apps, APIs, and Portal.

Sylton International makes use of “Private Label Sellers”: companies that sell the Sylton products and services under their own distinctive label. For customers subscribing to our services through a Private Label Seller, please note your information will be shared with this Private Label Seller and this information will be subject to the policies and terms of this Private Label Seller. A list of Sylton’s Private Label Sellers is attached to the Sylton Connect Terms & Conditions as addendum D.

Topics Covered:

---

1. What Data Do We Collect?

Business Data:

- Personal Identification Information: Includes first name, last name, email address.
- Device and Usage Information: Includes browser/app version, device identifiers, account actions (e.g., sharing, editing, viewing sessions), and usage metrics (e.g., patient counts, consultation details, angles shot, light modes used).
- Company Information: Includes address, employee count, branch locations, market segment, most popular treatments.
- Payment Data: Includes names and credit card details.
- Communication Logs: Includes records of interactions with us.

Patient Data:

- Personal Identification Information: Includes first name, last name, birthdate, gender, email address, phone number, address.
- Consultation Information: Includes dates, notes, images (e.g of the face, neck, hands and decollete), treatments, and prescribed products.

2. How Do We Collect Your Data?

Business Data is collected during*:*

- Business registration.
- User registration.
- Payment process.
- Consultation process.

Patient Data is collected during:

- Patient setup.
- Consultation process.

All data is stored on your device and automatically synchronized with Sylton Connect.

3. How Will We Use Your Data?

We process data for the following purposes, in compliance with GDPR:

Business Data (ref. section 1):

- For the performance of the contract (GDPR Article 6(1)(b)).
- To meet legal obligations (GDPR Article 6(1)(c)).
- To safeguard intellectual property, detect misuse, and troubleshoot issues (GDPR Article 6(1)(f)).
- For statistical analysis and scientific research (GDPR Article 6(1)(f))
- Marketing communications, with opt-out provisions (GDPR Article 6(1)(f)).

Patient Data (ref. section 1):

- We process your personal data as necessary for the performance of our contract with you ((GDPR Article 6(1)(b)), enabling you to provide care to your patients and ensuring your data is securely encrypted and stored for future reference.
- For statistical analysis and scientific research, with appropriate safeguards Article 9(2)(j)

4. How Do We Handle Patient Face data?

We handle face data with special care to protect privacy and comply with all legal requirements:

- *Purpose of Face Data:* Patient Face Data are processed exclusively to assist the clinic's practitioners in assessing skin conditions and recommending appropriate treatments. These images are *not* used for any other purpose (for example, they are not used for biometric identification or facial recognition).

- *Practitioner Control:* The clinic's practitioners have *full control* over the storage of patient Face Data in Sylton Connect. You (the practitioner or clinic) can delete any patient face photograph at any time via the Sylton Connect app or portal. When face data is deleted by the practitioner – it is immediately and permanently removed.
- *Face data Retention/Deletion Under Clinic Direction:* Face data are kept only as long as the clinic considers necessary for patient care. When face data is deleted by the practitioner – it is immediately and permanently removed. The clinic is responsible for ensuring data retention complies with relevant laws and guidelines.
- *Face data Retention/Deletion by us:* We do not store face data indefinitely or set retention periods; instead, we follow the clinic's instructions.
- *Processing of Face Data:* The app processes "Face Data" (e.g., facial geometry, face mesh, blend-shape values) only in volatile memory on device for real-time operation and does not retain this data.
- *No External Sharing:* We do *not* share patient face data with any third parties. Face Data remain within the Sylton Connect system under the clinic's control and are not disclosed to outside entities.
- *Secure Encrypted Storage:* The only external service involved is our secure cloud hosting provider, which stores the Face Data in encrypted form on our behalf *solely* to enable the Sylton Connect service. This provider cannot view or access the Face Data, and it does not process them for any independent purpose. In other words, even though the data is stored on a third-party server, it remains encrypted and inaccessible to that provider, and it is stored only for the duration necessary to support the Sylton Connect application.
- *Our Role as Data Processor:* When handling Face Data for patient care, we act strictly as a *data processor* on behalf of the clinic and its practitioners. This means we process and store these images only according to the clinic's instructions and for the purposes the clinic has determined (i.e., providing skincare consultations and treatment planning). We do not use these photos for any purposes of our own.
- *Our Role as Data Controller with Strict Safeguards:* When handling patient Face Data for broader statistical analysis or scientific research to improve our products and services, we act as the *data controller* for that specific processing. Any such use of face data for research is done in accordance with GDPR Article 9(2)(j), which permits processing of sensitive data for research purposes, and *is always subject to strict safeguards* per GDPR Article 89(1) and UAVG Article 44. In practice, this means:
    - *Pseudonymisation:* Before using face data for research, we replace or remove personal identifiers so individuals are not directly identifiable.
    - *Limited Re-Identification:* We implement measures to prevent the data from being linked back to specific patients during research. Any identifying details are kept separate to avoid re-identification.
    - *Security Measures:* We apply robust technical and organizational security controls to research data (such as encryption, secure storage, and access logging) to prevent unauthorized access or disclosure.

- *Restricted Access:* Only a very limited number of authorized personnel with a direct need (e.g., qualified researchers bound by confidentiality) can access the pseudonymised research data.
- *Ethical Oversight:* If applicable, any research involving patient data is subject to ethics and compliance review to ensure it meets legal and ethical standards.

5. With What Third Parties Is Your Data Shared?

Patient Data:
- Patient data (which includes face data) is not shared with third-parties.

Business Data:
- Dedicated Sylton Connect Partners for the technical and commercial support of the Sylton branded devices (GDPR Articles 6(1)(b) and 6(1)(f)). For customers subscribing to our services through a Private Label Seller, please note the technical and commercial support will be provided by the Private Label Seller.
- Payment service providers (GDPR Article 6(1)(b)).
- Credit reference agencies for fraud prevention (GDPR Article 6(1)(f)).
- Third parties under specific circumstances, such as for legal compliance, to protect the vital interests of the data subject or another natural person, for fraud prevention, or for tasks carried out in the public interest (GDPR Articles 6(1)(c), 6(1)(d), 6(1)(e), and 6(1)(f)).

6. Where Do We Store Your Data?

All data is stored in the country/region you select during Sylton Connect setup.

7. How Do We Store Your Data?

- Your data is hosted on AWS, utilizing advanced encryption (128-bit and 256-bit).
- Your data is encrypted end-to-end, both on devices and during transmission.
- Redundant storage across 2 to 4 separate locations ensures data availability.

8. How Long Do We Store Your Data?

Your business data is retained only as long as necessary for its intended purposes.

All Patient Data is retained under the clinic control.
- You can delete your information at any time in the app and portal
- Upon cancellation of your subscription.

Please Note:
- Encrypted disaster-recovery backups may persist for up to 12 months and are used solely to restore service, not for access or processing.
- Specific information may be retained to comply with legal obligations, resolve disputes, enforce agreements, or prevent harm.

9. How Do We Protect Your Data?

InnoFaith and Sylton International employ robust security measures, including:

- An ISO 27001-certified Information Security Management System (ISMS).
- Regular penetration testing and vulnerability assessments.
- Restricted system access with Multi-Factor Authentication for authorized personnel only.
- Logging and monitoring.
- Data encryption (128-bit and 256-bit).
- Comprehensive annual security and awareness training for staff.
- Confidentiality agreements embedded in employee contracts.

10. What Are Your Data Protection Rights?

You have the following rights:

- *Access*: Request copies of your personal data.
- *Rectification*: Correct or complete your data.
- *Erasure*: Request data deletion under certain conditions.
- *Restriction*: Object to data processing under certain conditions.
- *Consent Withdrawal*: Revoke consent for future data processing.
- *Portability*: Request data transfer to another organization.

Most rights can be exercised directly through the Sylton Connect portal. For other requests, please email privacy@innofaith.com or privacy@sylton.com and include identity verification. We will respond to your request within one month.

11. Changes to Our Privacy Notice

This Privacy Notice is reviewed regularly. Updates are published in the Sylton Connect portal.

12. How to Contact Us

InnoFaith and Sylton International are located at SciencePark 5204b, 5692EG, Son en Breugel, The Netherlands, and are registered with the Chamber of Commerce under number 17093863 and 86748696.

If you have any questions about this privacy notice, the data we hold on you, or if you would like to exercise your data protection rights, please contact our privacy manager at either privacy@innofaith.com or privacy@sylton.com.

You also have the right to file a complaint regarding our processing of your personal data with the appropriate data protection supervisory authority in your country.