



CliniBot Privacy Policy

Effective Date: August 2025

Controller: Smiles and Bliss Ltd (Company No. 11818854)

Registered Office: 22 Wenlock Road, London N1 7GU, United Kingdom

Data Protection Officer (DPO): hello@myclinibot.com

1. Introduction and Purpose

1.1 Smiles and Bliss Ltd ("**Smiles and Bliss**", "**we**", "**us**", or "**our**") respects your privacy and is committed to protecting your personal data.

1.2 This Privacy Policy explains how we collect, use, store and disclose personal data processed through **CliniBot** and **myCliniBot** (together, the "**Platform**").

1.3 The Platform helps dental professionals create **clinical notes**, **track patient treatment journeys**, and **generate secure electronic consent forms**.

It is not an Electronic Health Record (EHR) system and is not designed for long-term record storage.

1.4 Please read this policy carefully together with any other privacy notices or fair processing notices that may apply on specific occasions.

2. Controller and Roles

2.1 Smiles and Bliss Ltd is the **Controller** for all personal data processed via the Platform.

2.2 Dental clinics using CliniBot remain **independent controllers** of their patient data within their own systems. Smiles and Bliss acts as controller for data processed within the Platform only.

2.3 Clinics are responsible for exporting permanent patient records to their own EHR systems and for responding to data subject requests relating to those records.

2.4 You may contact our **Data Protection Officer (DPO)** at **hello@myclinibot.com** for any privacy-related enquiry.

2.5 You have the right to make a complaint to the **Information Commissioner's Office (ICO)** (www.ico.org.uk / 0303 123 1113), although we encourage you to contact us first.

3. Third-Party Links

Our websites or emails may contain links to third-party websites, plug-ins, or applications. Following those links may allow third parties to collect or share data about you. We do not control these websites and are not responsible for their privacy statements. We encourage you to read the privacy policy of every website you visit.

4. Scope of Processing

The Platform comprises three modules:

Module	Description	Retention
Notes Creator	Enables clinicians to create clinical notes. May include patient initials and clinical details entered by the user.	Automatically and irreversibly deleted within 48 hours .

Module	Description	Retention
Consent Forms	Generates and delivers secure e-consent forms via password-protected link to patients (8-digit DOB as password). Contains patient identifiers and clinician name.	Retained 11 years for adults or until age 25 for children , whichever is longer.
Patient Tracker	Allows clinics to record patient name, surname, DOB, and treatment journey progress.	Retained in line with the consent-form schedule.

Clinics should export all long-term records to their EHR systems.

5. Categories of Personal Data

We collect and process the following categories of data, depending on Platform use:

Category	Examples
Identity Data	Patient first name, surname, initials, date of birth, clinician name, GDC number, clinic name.
Contact Data	Patient and clinic email addresses (for consent delivery and audit trails).
Health Data	Treatment details and clinical notes entered by the clinician.
Technical Data	IP address, device type, browser information, timestamps, user agent strings (for security and audit).
Account Data	Clinician log-in credentials, role-based access, subscription details.
Audit Trail Data	Records of when a consent form was sent, viewed, and signed.
Financial Data	Limited to subscription payments for clinic users (processed via Stripe).

Audio/Transcription Data

When speech-to-text is used, **audio is processed transiently** by EU-based providers (Google Cloud, Azure, Assembly AI). No audio is stored by Smiles and Bliss after conversion. Only the resulting text output is retained, and in Notes Creator it is auto-deleted after 48 hours.

6. How We Collect Personal Data

- **Direct Input:** From clinics when entering patient details to generate consent forms or update treatment trackers.
- **Automated Collection:** Technical and audit data captured through secure logs (e.g., timestamps, IP).
- **No Third-Party Marketing Data:** We do not obtain data from external marketing lists or public sources for patient processing.

If You Fail to Provide Personal Data

Where provision of personal data is required by law or under a contract with your clinic, failure to provide it may mean we cannot provide the relevant service. We will notify the clinic if this applies.

7. Purposes and Lawful Bases for Processing

Purpose	Lawful Basis (Article 6 UK GDPR)	Special Category Basis (Article 9)
Provide and operate the Platform (notes, consent, tracking).	Contract (6(1)(b))	Health care provision (9(2)(h))
Maintain security, logs and backups.	Legitimate interest (6(1)(f))	—
Fulfil legal and regulatory obligations (e.g., retention, DPA 2018).	Legal obligation (6(1)(c))	—
Manage user accounts, billing, and payments.	Contract (6(1)(b))	—
Communicate service updates or legal notices.	Legitimate interest / Legal obligation	—
Send optional marketing to clinics.	Consent (6(1)(a))	—

Change of Purpose

We will only use your data for the purposes set out above unless we reasonably consider another purpose compatible with the original. If processing for a new incompatible purpose is required, we will notify you and explain the lawful basis.

8. Marketing and Opt-Out

We may send service communications to clinic users (non-marketing).

We may send marketing communications to clinics with consent, which can be withdrawn at any time via the unsubscribe link or by contacting hello@myclinibot.com.

We do not send marketing to patients.

9. Automated Decision-Making

We do not use automated decision-making or profiling that produces legal or similarly significant effects. No behavioural or marketing profiling of patients occurs.

10. Data Retention and Deletion

Data Type	Retention Period	Deletion Method
Clinical Notes	48 hours from creation	Hard deleted from live and backup storage.
Consent Forms & Audit Trails	11 years from last entry (adults) / until age 25 (minors)	Secure erasure after expiry.
Patient Tracker Data	Same as consent forms	Secure erasure.
Billing & Account Data	7 years (tax/accounting)	Erasure or anonymisation.

Residual encrypted copies may persist temporarily in backup archives for disaster recovery and are purged in accordance with our rotation schedule.

11. Security Measures

We employ layered technical and organisational controls:

- **Encryption in Transit:** TLS 1.2+ with HSTS and HTTPS enforced.
- **Encryption at Rest:** AES-256 (Firebase / GCP).
- **Access Control:** Role-based permissions, SSO authentication (Firebase).
- **Document Security:** Single-use, time-limited tokens and DOB password for patient signature access.
- **Audit Trails:** Timestamped logs including IP and user agent.
- **Data Minimisation:** Patient initials only in Notes Creator (no full identifiers).
- **Error Logging:** Anonymous, structured logging via Sentry.
- **Regular Access Reviews:** Least-privilege principle.

12. International Data Transfers

12.1 All data is hosted and processed **within the EEA** (Frankfurt and Netherlands).

12.2 No transfers occur outside the UK / EEA.

12.3 If any future transfer is required, Smiles and Bliss will implement an appropriate safeguard (UK IDTA / EU SCCs), complete a transfer risk assessment, and update this Policy.

13. Disclosures and Sub-Processors

We share personal data only where necessary for Platform operation, under written Data Processing Agreements.

Sub-Processor	Purpose	Location
Google Cloud (Firebase)	Hosting / database	EU (Netherlands / Frankfurt)
Azure Speech to Text	Transcription (EU-only)	EU
Assembly AI	Speech to text processing	EU
SendGrid	Email delivery (consent links)	EU
Stripe	Payment processing	EU
Sentry	Anonymous error logging	EU
PDF Shift	PDF generation	EU

Law Enforcement Requests.

We may disclose data where required by law or valid legal process. Each request is assessed for scope and legality; we disclose the minimum necessary and, where lawful, notify the clinic concerned.

Professional Advisors and Authorities.

We may also share data with our legal, tax or insurance advisors, or with regulators such as HMRC or the ICO where legally required.

14. Cookies and Tracking

14.1 The Platform uses only **essential session cookies** required for secure login and operation.

14.2 No analytics, advertising or tracking cookies are used.

14.3 For full details see our [Cookie Policy](#) which complies with the **Privacy and Electronic Communications Regulations (PECR)**.

14.4 “Do Not Track” browser signals are honoured.

15. Your Rights under the UK GDPR

You have the right to:

- **Access** your data (subject access).
- **Rectify** inaccurate or incomplete data.
- **Erase** data where processing is unlawful or no longer required.
- **Restrict** processing in specific circumstances.
- **Object** to processing based on legitimate interests.
- **Data Portability** for information you provided electronically.
- **Withdraw Consent** where relied upon.

We respond within one month of verifying identity.

We may request ID before fulfilling a request and may charge a reasonable fee or refuse only if a request is manifestly unfounded, repetitive or excessive.

16. Children’s Data

Patient data relating to minors is processed solely for clinical purposes.

Records are retained **until the patient reaches age 25 or 11 years from the last entry**, whichever is longer, in accordance with NHS dental record retention guidance.

17. Data Breach Procedures

17.1 We maintain an incident-response plan to detect, investigate and remediate data breaches.

17.2 Where a breach is likely to result in a risk to individuals, we will notify the **ICO within 72 hours** and affected clinics or patients without undue delay.

17.3 Breach logs are retained for audit purposes.

18. International Operations and Future Changes

If we expand to new jurisdictions, we will ensure equivalent data protection standards, implement approved transfer mechanisms, and update this Policy accordingly.

19. Updates to this Policy

We may update this Privacy Policy periodically. The date above indicates the most recent revision. Material updates will be notified via email or the Platform dashboard.

20. Contact and Complaints

For any questions, concerns, or to exercise your rights, please contact:

Data Protection Officer – Smiles and Bliss Ltd

hello@myclinibot.com

22 Wenlock Road, London N1 7GU

You may also contact the **Information Commissioner's Office (ICO)** at www.ico.org.uk.

We encourage you to contact us first so we can resolve your concern promptly.