

SONÜ

Patient and Website Privacy Notice

How Dr. Alexander James Limited, trading as SONÜ Clinic, collects, uses, shares and protects personal information.

Effective date

31 July 2026

Next scheduled review

31 July 2027

Document owner

Clinic Manager / Privacy Lead

Classification

Public-facing

Applies to

Patients, prospective patients, treatment models, website users, visitors, callers, marketing subscribers, suppliers and job applicants.

Controller details

Dr. Alexander James Limited, trading as SONÜ Clinic
34 Hale Road, Hale, Cheshire, WA14 2EX
contact@sonuclinic.com • 01625 725 737
Company number 11579185 • ICO registration ZB356204

Important

This notice should be read alongside treatment consent, clinical photography consent, the Cookie Policy and any information provided at the point personal information is collected.

1. Who we are

Dr. Alexander James Limited, trading as SONÜ Clinic, is the data controller for the personal information described in this notice. We decide why and how that information is used.

Detail	Information
Legal name	Dr. Alexander James Limited
Trading name	SONÜ Clinic
Company number	11579185
ICO registration	ZB356204
Address	34 Hale Road, Hale, Cheshire, WA14 2EX
Telephone	01625 725 737
Email	contact@sonuclinic.com
Websites	sonuclinic.com and doctoralex.co.uk

2. Who this notice covers

This notice applies when you enquire about, book, receive or discuss treatment with us; participate as a treatment model; attend training or educational activity; use either website; visit our premises; communicate with us; subscribe to marketing; apply for work; or otherwise deal with the clinic.

We do not treat anyone under 18. If a person under 18 contacts us, we use only the information reasonably required to respond and manage the enquiry appropriately.

3. Personal information we collect

- Identity and contact details, including name, address, date of birth, telephone number, email address, sex or gender, occupation, emergency contact details and, where appropriate, photographic identification or proof of age.
- Health and clinical information, including medical history, conditions, medication, allergies, previous procedures, suitability assessments, consultation notes, diagnoses, prescriptions, treatment records, product and batch details, quantities used, aftercare, outcomes, complications and adverse events.
- Clinical photographs and video, including full images retained as part of the clinical record and versions authorised for marketing, education, training or case studies.
- Appointment and account information, including bookings, attendance, correspondence, invoices, refunds and transaction records. Full card details are generally handled by Stripe or Clover rather than stored by us.

- Communications, including emails, SMS, WhatsApp, social-media messages, website enquiries, notes of conversations, selected call recordings and AI-generated notes or summaries.
- Website and device information, including IP address, device and browser information, cookie identifiers, pages visited and website interactions, where permitted by your cookie choices.
- CCTV images when you visit or pass through areas covered by our surveillance system.
- Complaint, incident and legal information, including correspondence with insurers, solicitors, regulators, professional bodies and law-enforcement authorities.
- Recruitment and business-contact information, including CVs, qualifications, employment history, references and information supplied by applicants, suppliers or professional contacts.

4. How we obtain information

We usually obtain information directly from you through Pabau forms, bookings, consultations, treatment records, websites and communications. We may also receive information from:

- another clinic or healthcare professional making a referral;
- a person acting with your authority;
- pharmacies, laboratories, product suppliers or organisations supporting your treatment;
- payment, identity, fraud-prevention, website, communications or IT providers; and
- publicly available sources where reasonably necessary for recruitment, business administration or legal matters.

We sometimes record GP details but do not routinely send information to a GP. We may contact or disclose information to another healthcare professional where you ask us to do so, where necessary for your care, or where another lawful and ethically appropriate reason applies.

5. Why we use information and our lawful bases

We use personal information only where a lawful basis applies under Article 6 of the UK GDPR. When we use health information or other special-category information, we also identify an Article 9 condition and any relevant condition under the Data Protection Act 2018.

Purpose	Use	Lawful basis
Enquiries, bookings and treatment	Respond to enquiries, assess suitability, book appointments, provide consultations and treatment, prescribe or obtain products, provide aftercare and maintain an accurate clinical record.	Contract or steps before contract; legitimate interests. Health data: health care or treatment; legal claims where relevant.
Patient safety and clinical governance	Check contraindications, monitor results, investigate complications, trace products and batch numbers, audit care and improve standards.	Legitimate interests; legal or professional obligations. Health data: health care or treatment; legal claims.
Payments and accounts	Take payment, issue invoices and refunds, recover debts and keep tax and accounting records.	Contract; legal obligation; legitimate interests.
Communications, calls and AI notes	Communicate, preserve important discussions, confirm instructions or consent, support quality assurance and handle concerns.	Contract; legitimate interests; legal claims. Health data: health care or treatment; legal claims.
Clinical photography	Assess, plan, document and monitor treatment as part of the confidential clinical record.	Contract; legitimate interests. Health data: health care or treatment; legal claims.
Marketing, publication, education and training	Send marketing where permitted and use images or case material for the specific secondary purposes selected.	Consent. Health information or identifiable clinical imagery: explicit consent.

Purpose	Use	Lawful basis
Websites and analytics	Operate and secure the websites, remember essential choices and understand use of the sites.	Legitimate interests for essential functions; consent for non-essential cookies and analytics.
CCTV	Protect people and property and investigate accidents, crime, misconduct or disputes.	Legitimate interests; legal claims.
Complaints, insurance and legal matters	Investigate, respond, notify insurers, obtain advice and establish, exercise or defend legal claims.	Legal obligation; legitimate interests; legal claims.
Recruitment and administration	Assess applicants, employ staff, manage suppliers and run the business.	Steps before contract; contract; legal obligation; legitimate interests.

6. Clinical photographs, video and consent

We routinely take full clinical photographs where reasonably required to assess suitability, plan treatment, document what was provided, monitor progress and protect patient safety. Those photographs form part of the confidential clinical record even where you permit no marketing or publication.

At each relevant appointment, the consultation and consent process allows you to choose whether secondary use is permitted. Options may include uncensored use, censored or de-identified use, or no secondary use. Training and educational use is censored where that is the choice and wording presented to you.

You may withdraw consent for future marketing, publication, education or training use at any time. We will stop new use and take reasonable steps regarding material under our control. Withdrawal does not make earlier lawful use unlawful, cannot always retrieve material already printed or shared by others, and does not normally require deletion of the confidential clinical record.

Clinical photographs are stored within Adobe Creative Cloud under a business account in the company name. Some, but not all, are also stored in Pabau. Access is restricted to authorised staff.

7. Telephone calls and AI-assisted notes

We use RingCentral. Selected calls may be recorded and may be transcribed or summarised using RingCentral AI Assistant. Callers are informed where recording or AI-assisted note-taking applies. Calls may contain health information, treatment concerns, adverse events, consent discussions or other sensitive information.

AI outputs are treated as drafts. Staff review relevant content before relying on it or adding it to Pabau. We do not use call recordings or AI notes to make solely automated treatment decisions that have legal or similarly significant effects.

8. Marketing

We may send marketing by email, SMS, WhatsApp, telephone or post only where an appropriate consent or other lawful permission applies. Our usual approach is an active opt-in. We do not add someone to electronic marketing merely because they made an enquiry.

You can change preferences through the Pabau portal, use an unsubscribe facility where available, or contact us. We may keep a minimal suppression record to ensure that an opt-out is respected. We do not upload patient lists to Google or Meta to create advertising or lookalike audiences, and we do not currently use retargeting pixels.

9. Who we share information with

- Pabau for booking, consultation forms and patient-management services;
- Stripe and Clover for payment processing;
- Microsoft 365, Google services and Adobe Creative Cloud for communications, files and business systems;
- RingCentral for telephony, selected call recording and AI-assisted notes;
- KDA Web Services and other website, hosting, maintenance, cybersecurity and IT providers;
- Xero, accountants and financial advisers;
- Healthxchange, Wigmore, John Bannon, MedFx, Roseway Labs and other pharmacies, laboratories or suppliers supporting prescriptions, dispensing or treatment;
- Meta platforms, including Facebook, Instagram and WhatsApp Business, where you communicate with us or consent to relevant activity;
- authorised trainers, delegates, representatives, manufacturers or professional audiences only where specific consent or another clear lawful basis applies;
- employees, insurers, solicitors, professional advisers, regulators, professional bodies, law-enforcement authorities and courts where necessary; and
- a purchaser, investor, lender or successor organisation if the business or assets are reorganised, financed, transferred or sold, subject to safeguards.

We do not sell patient information or disclose patient lists to advertisers.

10. International processing

Clinic staff access patient systems from the United Kingdom. Some technology, communications, analytics, payment or cloud suppliers may use international infrastructure or support teams. Where a restricted transfer occurs, we require a lawful transfer mechanism and appropriate safeguards, which may include UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum or the UK Extension to the EU-US Data Privacy Framework.

11. Security

- role-based access and individual user accounts;
- multi-factor authentication on key systems;
- business cloud accounts and no routine paper clinical files;
- staff confidentiality and data-protection duties;
- controlled access to Pabau, Adobe Creative Cloud, Microsoft 365 and payment systems;
- local, password-protected UniFi Protect CCTV storage;
- device, password, update, backup and incident-management controls; and
- supplier contracts and due-diligence checks where required.

12. CCTV, websites and cookies

CCTV

CCTV operates for safety, security, crime prevention and incident investigation. Footage is stored locally through UniFi Protect. It is not used for facial recognition or solely automated decisions. Routine footage is retained for up to 90 days; relevant footage may be isolated for longer for an incident, complaint, insurance matter or legal proceedings.

Websites and cookies

Our websites use essential technologies required for operation and security. Google Analytics and any other non-essential technologies are used only in accordance with the choices offered through the cookie banner.

You can reject non-essential cookies and change your choice later. See the separate Cookie Policy and live cookie settings for details.

13. Retention

We retain information only for as long as reasonably necessary, taking account of patient safety, treatment traceability, professional duties, limitation periods, complaints and claims, sensitivity and risk. Long retention is reviewable and must remain justified.

Information	Retention approach
Adult clinical records and clinical photographs	Normally retained for at least 20 years after the last treatment or meaningful clinical contact. After that point they are reviewed at least every five years and may be retained for the patient's lifetime or longer where a documented need remains, including safety, traceability, ongoing care, a serious incident, complaint, regulatory matter or legal claim.
Ordinary enquiries not leading to treatment	Normally 2 years. An enquiry containing material clinical advice, a complication, consent evidence, complaint or potential claim may be retained for up to 10 years or transferred to the clinical or complaint record.
Selected calls and AI notes	Up to 10 years where relevant to treatment, consent, quality assurance, a complaint, incident or legal claim. Duplicates or routine material may be deleted earlier.
Marketing consent and preferences	While active and up to 10 years after the last use, withdrawal or objection where required as compliance evidence. Minimal suppression information may be retained for as long as necessary to honour an opt-out.
Financial records	10 years from the end of the relevant financial period, or longer where required for an active audit or dispute.
CCTV	Up to 90 days on a rolling basis unless isolated for an incident or legal matter.
Complaints, incidents and claims	10 years after closure, or longer while active or reasonably anticipated.
Unsuccessful job applications	12 months after the decision unless the applicant agrees to longer retention or a dispute requires it.

14. Your rights

- access personal information we hold about you;
- correct inaccurate or incomplete information;
- request erasure where there is no overriding reason to retain it;
- request restriction of processing;
- object to legitimate-interests processing and object at any time to direct marketing;
- receive certain information in a portable format;
- withdraw consent at any time where processing relies on consent; and
- request information about relevant international-transfer safeguards.

These rights are not absolute. Clinical records may need to be retained despite an erasure request where they remain necessary for safety, professional duties or legal claims. Send requests to contact@sonuclinic.com. We normally respond within one month after receiving any information reasonably required to verify identity or clarify the request. A permitted extension may apply to complex or multiple requests.

15. Questions and data-protection complaints

Please contact the Privacy Lead at contact@sonuclinic.com or 34 Hale Road, Hale, Cheshire, WA14 2EX. We provide a clear route for data-protection complaints, acknowledge a complaint within 30 days, investigate it without undue delay, keep the complainant informed where appropriate and communicate the outcome.

You may also complain to the Information Commissioner's Office. The ICO recommends raising the matter with us first so that we have the opportunity to address it.

[Information Commissioner's Office - make a complaint](#) • Helpline 0303 123 1113

16. Changes to this notice

We may update this notice to reflect changes in law, guidance, treatments, systems, suppliers or our use of personal information. The current version will be published on both websites. Material changes may also be brought directly to the attention of affected people.

Legal framework and guidance

This document has been prepared with reference to the following legislation and official guidance, as available on the effective date:

- [ICO: A guide to the data protection principles](#)
- [ICO: Right to be informed](#)
- [ICO: Special category data](#)
- [GMC: Confidentiality - good practice in handling patient information](#)
- [Data Protection Act 2018](#)
- [Data \(Use and Access\) Act 2025](#)
- [ICO: How to deal with data protection complaints](#)
- [ICO: International transfers](#)