MyKneeScan

Privacy Policy

Version 2.0

Effective date: 1 May 2026

Website: mykneescan.com

ICO Reg: ZB123456

This is Version 2.0 of the MyKneeScan Privacy Policy, effective 1 May 2026. It supersedes Version 1.0 in its entirety. Key changes from v1.0 include: accurate description of MyKneeScan's role as a marketplace and clinical governance platform (not a direct clinical provider); clarified controller and processor responsibilities; specific data retention periods; strengthened Article 9 lawful basis; updated third-party recipient list including the Clinical Advisory Panel; data breach notification rights; and explicit exclusion of under-18s from self-referral services.

At a Glance	Detail
Data controller	MyKneeScan Ltd (subsidiary of SportsHealing Holdings)
Registered office	Woodlands Grange, Woodlands Lane, Bradley Stoke, Bristol, BS32 4JY
Privacy contact	info@mykneescan.com
Complaints	info@mykneescan.com
ICO registration	ZB123456
DPO	Appointed — contact via info@mykneescan.com
Telephone	020 7483 5160
Effective date	1 May 2026
Review date	1 May 2027

1. Who We Are

MyKneeScan is a digital marketplace and clinical governance platform that connects patients to vetted private imaging providers for knee MRI and musculoskeletal ultrasound in the United Kingdom. MyKneeScan does not itself perform imaging or provide direct clinical treatment. Our role is to:

- Facilitate the booking of knee imaging appointments with vetted network providers
- Conduct independent clinical vetting of scan requests through our Clinical Advisory Panel
- Set, monitor, and enforce the quality standards that listed providers must meet
- Deliver structured scan reports to patients on behalf of reporting radiologists
- Provide patient-facing educational content, triage tools, and risk assessment instruments

MyKneeScan is a subsidiary of SportsHealing Holdings. The platform is clinically governed by an Associate Professor of Knee Surgery and a Consultant Knee Radiologist, both acting as members of the MyKneeScan Clinical Advisory Panel.

Role	Detail
Data controller	MyKneeScan Ltd, a subsidiary of SportsHealing Holdings
Registered office	Woodlands Grange, Woodlands Lane, Bradley Stoke, Bristol, BS32 4JY
Privacy contact	info@mykneescan.com | 020 7483 5160
ICO registration number	ZB123456
Data Protection Officer	Appointed. Contact via info@mykneescan.com

Important — MyKneeScan's role as a marketplace: When you book a scan through MyKneeScan, your imaging appointment is performed by an independent vetted scanning provider, not by MyKneeScan. That provider is a separate data controller for the data they process in delivering your scan. This policy explains what data MyKneeScan processes and why. The scanning provider's own privacy notice governs their processing of your data.

2. Scope of This Policy

This policy explains how MyKneeScan collects, uses, shares, and protects your personal data when you:

- Use our website (mykneescan.com) or mobile application
- Book an imaging appointment through the MyKneeScan platform
- Complete the MyKneeScan Scan Vetting Pro Forma (Form MKS-VF-001)
- Use the KneeScore triage tool or any other risk calculator on the platform (note: no data from these tools is stored or transmitted — they are for your indicative use only)
- Upload documents such as MRI reports, referral letters, or clinical correspondence
- Communicate with us by phone, email, SMS, or online chat
- Receive your scan report or onward pathway recommendation through the platform

This policy does not cover:

- The data processing activities of independent vetted scanning providers, who have their own privacy notices
- Third-party websites that we link to from our platform

This service is for adults aged 18 and over only. MyKneeScan does not accept self-referrals from patients under the age of 18 through this platform. If you are under 18, please speak to your GP or parent/guardian, who can arrange appropriate clinical referral through NHS or private paediatric pathways. Any booking made on behalf of a person under 18 will be cancelled and refunded.

3. The Information We Collect

A) Identity and Contact Details

- Full name, date of birth, biological sex at birth (for clinical interpretation purposes)
- Email address, telephone number, address, and postcode
- Occupation and activity level (provided voluntarily as clinical context)

B) Booking and Service Information

- Appointment type, date, time, and location
- Booking reference numbers and booking history
- Correspondence relating to your booking — messages, call logs, and notes
- Payment status, invoice, and receipt references (not full card details — see Section 3D)

C) Health Information (Special Category Data)

Health data is special category data under Article 9 UK GDPR and receives the highest level of legal protection. We collect only the health information that is necessary for the specific purpose described. We never use your health data for advertising targeting or commercial profiling.

Health information we may collect includes:

- Knee symptoms, pain history, and mechanism of injury as described in the Scan Vetting Pro Forma
- MRI safety screening information — for example: implants, pacemaker status, pregnancy status, contrast allergies, claustrophobia
- Previous imaging results, referral letters, and clinical correspondence you choose to upload
- Surgical history relevant to knee imaging interpretation
- Current medications relevant to your clinical presentation
- Clinical notes and vetting assessment records created by the Clinical Advisory Panel
- Scan reports, imaging findings, and management pathway recommendations

D) Payment Information

- Payment status, payment reference IDs, and transaction records
- Invoice and receipt records retained for accounting and tax purposes

We do not store full card numbers. All card payment processing is handled by our payment provider (see Appendix A). We receive only a tokenised payment confirmation.

E) Risk Calculator and Triage Tool

The KneeScore risk calculator and any other triage tools on the MyKneeScan platform are provided for indicative purposes only, to help you decide whether to book a scan. We do not store, retain, or process the responses you enter or the score generated. Results are displayed to you in-session only and are not saved to any database, transmitted to our servers, or linked to your identity. No personal data is collected through the triage tool.

F) Website and Device Information

- IP address, browser type, and device identifiers
- Page visits, interactions, and navigation patterns
- Cookie and consent preferences

See Section 11 (Cookies) for full details.

4. How We Collect Your Information

We collect information in the following ways:

Source	Information Collected
Directly from you	Booking forms, the Scan Vetting Pro Forma (MKS-VF-001), document uploads, phone calls, emails, and online chat. Note: the KneeScore triage tool does not transmit or store any data — it operates entirely within your browser session.
Clinical Advisory Panel	Vetting assessment records, protocol modification notes, and clinical governance decisions made in reviewing your scan request
Vetted scanning providers	Scan completion confirmation, report delivery, and any clinical concerns identified at the time of your scan (limited to what is necessary for report delivery and governance)
Our technology suppliers	Booking system data (Semble), hosting infrastructure (Google Cloud Platform — UK region only), payment confirmation tokens, and analytics data where consented
Cookies and similar technologies	Website interaction data where you have consented to non-essential cookies (see Section 11)

5. Why We Use Your Information (Purposes)

Purpose	Data Used	Lawful Basis (see Section 6)
Booking management — confirming, managing, and communicating about your appointment	Identity, contact details, booking information	Contract (Art. 6(1)(b))
Clinical vetting — assessing whether your scan request is clinically appropriate	Health data from Scan Vetting Pro Forma (MKS-VF-001) only. Triage tool responses are not stored or transmitted.	Health/social care (Art. 9(2)(h) + DPA 2018 Sch.1) + Explicit consent (Art. 9(2)(a))
MRI safety screening — ensuring it is safe for you to undergo	Safety screening responses from pro forma	Health/social care (Art. 9(2)(h)) + Vital interests (Art. 9(2)(c)) where applicable

imaging		
Scan report delivery — transmitting your imaging report and management recommendations	Health data, imaging reports, contact details	Contract (Art. 6(1)(b)) + Health/social care (Art. 9(2)(h))
Payment processing and billing	Payment references, booking details	Contract (Art. 6(1)(b))
Accounting and tax compliance	Transaction records	Legal obligation (Art. 6(1)(c))
Clinical governance and quality audit — anonymised review of scan quality and report standards	Anonymised DICOM images and reports only — no identifiers	Legitimate interests (Art. 6(1)(f)) — quality assurance of a healthcare platform
Urgent clinical communication — contacting your GP if an urgent or incidental finding is identified	Limited health data, GP contact details if provided	Vital interests (Art. 6(1)(d)) + Art. 9(2)(c)
Customer support and complaints	Contact details, correspondence, booking records	Contract (Art. 6(1)(b)) + Legal obligation (Art. 6(1)(c))
Platform improvement and analytics	Anonymised/aggregated usage data; website analytics where consented	Legitimate interests (Art. 6(1)(f)) + Consent (Art. 6(1)(a)) for non-essential analytics
Marketing communications	Contact details — only where explicit opt-in consent given	Consent (Art. 6(1)(a)) — PECR compliant
Legal and regulatory compliance	Any data necessary to respond to regulatory requests or defend legal claims	Legal obligation (Art. 6(1)(c)) + Legitimate interests (Art. 6(1)(f))

6. Our Lawful Basis for Processing

A) Article 6 Lawful Bases (Personal Data)

Basis	When We Rely on It
Contract — Art. 6(1)(b)	Processing necessary to provide the booking and report delivery service you have requested. Applies to all core operational processing.
Legal obligation — Art.	Processing required to comply with legal duties, including

6(1)(c)	accounting, tax, and regulatory obligations.
Vital interests — Art. 6(1)(d)	Applied in exceptional circumstances only — where processing is necessary to protect your life or safety, for example communicating an urgent incidental finding.
Legitimate interests — Art. 6(1)(f)	Service improvement, fraud prevention, platform security, and anonymised quality audit. We have conducted a Legitimate Interests Assessment (LIA) for each use. Your rights do not override these interests in the assessed scenarios.
Consent — Art. 6(1)(a)	Non-essential cookies and direct marketing communications. You may withdraw consent at any time without affecting the lawfulness of prior processing.

B) Article 9 Conditions (Special Category Health Data)

Processing of your health data requires both an Article 6 lawful basis (above) and a separate Article 9 condition. We rely on the following Article 9 conditions:

Article 9 Condition	Application
Art. 9(2)(a) — Explicit consent	Obtained via the Scan Vetting Pro Forma consent section for all health data submitted at booking. Consent is granular, freely given, specific, and informed. You may withdraw consent at any time, subject to Section 14.
Art. 9(2)(h) — Health or social care purposes (+ DPA 2018 Schedule 1, Part 1, para. 2)	Processing necessary for the provision of health care and the management of health care systems — specifically: clinical vetting of scan requests, safety screening, report delivery, and clinical governance. Processing is carried out under a duty of confidentiality.
Art. 9(2)(c) — Vital interests	Applied in exceptional circumstances only, where processing is necessary to protect your vital interests and you are physically or legally incapable of giving consent — for example, in a medical emergency arising from a scan.
Art. 9(2)(j) — Archiving, research, and statistics	Applied to anonymised aggregate data only, for the purpose of improving clinical quality across the platform. No identifiable data is used for this purpose.

We do not use your health data for advertising targeting, commercial profiling, or any purpose other than those listed in this section. Health data is never sold, licensed, or shared with third parties for commercial gain.

7. Who We Share Your Information With

We share personal data only where necessary for a specific, identified purpose. We apply a minimum necessary data principle — we share only the information required for each recipient's specific role.

A) MyKneeScan Clinical Advisory Panel

The Associate Professor of Knee Surgery and Consultant Knee Radiologist who form the Clinical Advisory Panel access your Scan Vetting Pro Forma data and (for audit purposes) anonymised scan data in order to conduct clinical vetting assessments and quality reviews. Both panel members are bound by professional confidentiality obligations and contractual data processing agreements with MyKneeScan.

B) Vetted Scanning Providers

When your scan request is approved, your booking details and the clinically relevant information from your Scan Vetting Pro Forma are shared with the vetted scanning centre at which your appointment is booked. This information enables the scanning centre to prepare the correct imaging protocol and conduct their own safety screening prior to your appointment.

The vetted scanning provider is an independent data controller for the personal data they process in delivering your scan. MyKneeScan shares only the minimum information necessary. You should request the scanning provider's own privacy notice at the time of your appointment. MyKneeScan is not responsible for the scanning provider's data handling beyond the obligations set out in the MyKneeScan Provider Agreement.

C) Reporting Radiologist

The reporting radiologist at the scanning centre receives your scan images and the relevant clinical context from your pro forma in order to produce your report. The reporting radiologist acts under the governance of both the scanning provider and the MyKneeScan quality framework.

D) Your GP or Referring Clinician

We will share information with your GP or referring clinician only in two circumstances: (1) where you have explicitly requested that your report be forwarded to them; or (2) where the vetting clinician or reporting radiologist identifies an urgent or clinically significant finding that, in their professional judgement, requires prompt GP notification in your interest. In the second case, we will inform you that this communication has taken place.

E) Technology and Service Suppliers (Processors)

We use a limited number of suppliers who process personal data on our behalf as data processors under formal Data Processing Agreements. Current key processors are listed in Appendix A. All processors are contractually required to:

- Process data only on MyKneeScan's documented instructions
- Implement appropriate technical and organisational security measures
- Not engage sub-processors without MyKneeScan's prior written consent
- Delete or return data on termination of the relationship
- Cooperate with data protection audits and inspections

F) Legal and Regulatory Recipients

We may share information with regulators (including the ICO, CQC, or MHRA), law enforcement agencies, courts, or legal advisers where required by law or where necessary to establish,

exercise, or defend legal claims. We will notify you of such disclosure unless legally prohibited from doing so.

G) Sharing at Your Request

If you ask us to share your scan report or clinical information with a third party — for example a physiotherapist, sports medicine doctor, orthopaedic surgeon, or insurer — we will do so following appropriate identity verification and will record your instruction.

8. Hosting and International Data Transfers

All patient personal data and health data processed by MyKneeScan is hosted and processed exclusively within the United Kingdom, using Google Cloud Platform infrastructure in the UK (eu-west-2 / London region). We do not store patient data in EEA or other international locations.

Where any supplier processes data outside the UK, we require:

- A Transfer Risk Assessment (TRA) to be completed prior to any transfer
- Appropriate safeguards to be in place — either UK adequacy regulations, a UK International Data Transfer Agreement (IDTA), or a UK Addendum to EU Standard Contractual Clauses
- The transfer to be listed in Appendix A with the applicable safeguard identified

Note on US-owned processors: MyKneeScan uses Google Cloud Platform (a US-owned service) with data stored in UK regions only. We have assessed the risk of potential US law enforcement access under the CLOUD Act and FISA authorities. Given the nature of the data processed and the UK-only storage configuration, we consider the residual transfer risk to be low. A Transfer Risk Assessment is maintained and reviewed annually.

9. How Long We Keep Your Information

We retain personal data only for as long as necessary for the purposes described in this policy and to meet applicable legal and clinical governance obligations. Our retention schedule is as follows:

Record Type	Retention Period	Basis
Adult clinical records, scan reports, and imaging (patients aged 18+)	8 years from last episode of care	NHS Records Management Code of Practice 2021
Scan Vetting Pro Forma (MKS-VF-001)	8 years from completion	NHS Records Management Code of Practice 2021
Booking and administrative records	8 years from last episode (aligned to clinical record)	Consistency with clinical record retention
Billing and accounting records	6 years from financial year end	Companies Act 2006 / HMRC requirements
Marketing consent records	Duration of consent	ICO guidance on consent records

	+ 1 year after withdrawal	
Website analytics data	14 months maximum	Standard analytics practice; Google Analytics default
Audit logs and security logs	12 months rolling	Security monitoring and incident investigation
Complaint and incident records	8 years	Clinical governance and legal claims limitation
Anonymised quality audit data	Indefinite (no retention limit applies to anonymised data)	Not personal data once fully anonymised

At the end of the applicable retention period, personal data is securely deleted or anonymised. We do not retain data speculatively or beyond the purposes for which it was collected.

10. Security and Confidentiality

We implement technical and organisational measures proportionate to the risk of processing special category health data. Our security controls include:

Control	Implementation
Encryption in transit	TLS 1.3 for all data transfers between users, the platform, and partner systems
Encryption at rest	AES-256 encryption for all stored patient and clinical data; keys managed via dedicated key management service
API authentication	OAuth 2.0 with short-lived access tokens; no static API keys or shared passwords
Access controls	Role-based access control (RBAC); minimum necessary access principle applied to all staff and system roles; multi-factor authentication required for all staff accessing health data
Audit logging	All data access events logged with timestamp, user identity, and action; logs retained for 12 months
Penetration testing	Annual independent penetration test by a CREST-accredited provider; findings remediated within agreed timescales
Staff training	All staff with access to personal data complete data protection training at induction and annually thereafter
Supplier due diligence	All processors assessed for security standards before engagement; Data Processing Agreements in place
ISO 27001 alignment	Information security management practices aligned with ISO 27001; formal certification in progress

No digital system is completely immune from security risk. In the event of a personal

data breach that is likely to result in a high risk to your rights and freedoms, we will notify you without undue delay and, where required, notify the ICO within 72 hours of becoming aware of the breach. If you suspect your data may have been compromised, contact us immediately at info@mykneescan.com.

11. Cookies and Similar Technologies

We use cookies and similar technologies on our website. Under UK PECR, non-essential cookies require your informed opt-in consent before they are placed.

Cookie Category	Purpose	Consent Required?
Strictly necessary	Essential for the website to function — for example session management, security tokens, booking flow continuity. Cannot be disabled.	No
Functional	Remember your preferences and settings to improve your experience — for example saved location or booking history.	Yes
Analytics	Understand how visitors use our website to improve performance and content. We use anonymised or pseudonymised data only.	Yes
Marketing	Only used if you have explicitly opted in to marketing communications. Not used for health data targeting.	Yes

You can manage your cookie preferences at any time using the cookie settings tool on our website. Withdrawing consent for non-essential cookies does not affect your ability to book a scan or use the core platform.

12. Marketing Communications

MyKneeScan may send you marketing communications about our services, content, or relevant offers — but only if you have given explicit opt-in consent through the Scan Vetting Pro Forma or another clearly presented consent mechanism. The lawful basis for all marketing communications is consent (Article 6(1)(a) UK GDPR), in compliance with UK PECR.

We will never:

- **Use your health data for marketing targeting or segmentation**
- Send marketing communications based on legitimate interests (not valid for direct marketing under PECR)
- Share your contact details with third parties for their marketing purposes

You can withdraw your marketing consent at any time by:

- Clicking the unsubscribe link in any marketing email
- Contacting us at info@mykneescan.com
- Updating your preferences in your MyKneeScan account settings

Operational messages — appointment confirmations, safety instructions, vetting decisions, and report delivery notifications — are sent without requiring marketing consent, as they are necessary to deliver the service you have contracted for.

13. Automated Decision-Making and AI Tools

A) KneeScore and Risk Calculator

The KneeScore triage tool and knee health risk calculator on the MyKneeScan platform use automated scoring logic to generate an indicative risk score and scan recommendation based on your responses. This output is displayed to you in-session only to help you decide whether to book a scan. We do not store, retain, or transmit your responses or your score — no data from the triage tool is saved to our systems or shared with the vetting clinician.

> The KneeScore output is not a clinical diagnosis. It is an educational and navigational tool designed to help you understand whether an MRI or ultrasound scan may be appropriate for your symptoms. The clinically binding decision on whether your scan proceeds is made by the MyKneeScan Consultant Knee Radiologist through the vetting process — not by the automated tool.

The KneeScore tool does not constitute automated decision-making with legal or similarly significant effects under Article 22 UK GDPR, because it does not determine whether your scan proceeds — that decision is made by a qualified clinician. However, if you wish to query the output of the risk calculator, you may contact us at info@mykneescan.com.

B) Report Explanation Tools

MyKneeScan may use AI-assisted tools to generate plain-English summaries of imaging reports to help patients understand clinical findings. These summaries:

- Are generated in addition to, not in place of, the clinical report produced by the reporting radiologist
- Are clearly labelled as AI-generated plain-language summaries
- Are not clinical diagnoses and do not constitute medical advice
- Are reviewed by the platform's clinical governance process before delivery

C) No Solely Automated Decisions with Significant Effects

MyKneeScan does not make any decision that produces legal or similarly significant effects for you based solely on automated processing without human oversight. All clinically significant decisions — including vetting approval, non-approval, and protocol modification — are made by a qualified clinician.

14. Your Rights Under UK GDPR

Right	What It Means	How to Exercise It
Right of access (Art. 15)	Request a copy of the personal data we hold about you.	Contact info@mykneescan.com. We will respond within one month.

Right to rectification (Art. 16)	Request correction of inaccurate or incomplete data.	Contact info@mykneescan.com.
Right to erasure (Art. 17)	Request deletion of your data in certain circumstances — for example where processing was based on consent that you have withdrawn.	Contact info@mykneescan.com. Note: we may be unable to delete clinical records where retention is required by law or clinical governance obligations.
Right to restrict processing (Art. 18)	Request that we limit how we use your data in certain circumstances — for example while a correction is being assessed.	Contact info@mykneescan.com.
Right to data portability (Art. 20)	Receive a copy of data you have provided to us in a structured, commonly used, machine-readable format, where processing is based on consent or contract.	Contact info@mykneescan.com.
Right to object (Art. 21)	Object to processing based on legitimate interests. We will cease processing unless we can demonstrate compelling legitimate grounds that override your interests.	Contact info@mykneescan.com.
Right to withdraw consent (Art. 7(3))	Withdraw consent for consent-based processing (including marketing and non-essential cookies) at any time. Withdrawal does not affect the lawfulness of prior processing.	Unsubscribe link, cookie settings, or info@mykneescan.com.
Rights related to automated decision-making (Art. 22)	Request human review of any automated decision that significantly affects you, and to express your point of view.	Contact info@mykneescan.com.

Some rights are not absolute and may be limited where we are required to retain records for legal, regulatory, or clinical governance reasons. We will always explain if we are unable to fulfil a rights request and why.

To exercise any right, contact us at info@mykneescan.com. We may need to verify your identity before actioning your request. We will respond within one calendar month. Complex requests may be extended by a further two months with notification.

15. Data Breach Notification

In the event of a personal data breach, MyKneeScan will:

- Assess the risk to individuals' rights and freedoms without undue delay
- Notify the ICO within 72 hours of becoming aware of a breach that is likely to result in a risk to individuals' rights and freedoms

- Notify affected individuals directly and without undue delay where the breach is likely to result in a high risk to their rights and freedoms

Notification to individuals will include:

- A description of the nature of the breach
- The name and contact details of our Data Protection Officer
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to address the breach

If you suspect that your personal data has been compromised, or if you receive a suspicious communication that appears to be from MyKneeScan, please contact us immediately at info@mykneescan.com or info@mykneescan.com.

16. Complaints

If you are unhappy with how we have handled your personal data, please contact us first so that we can investigate and seek to resolve your concern:

Contact Route	Address	Response Time
Privacy / data protection concern	info@mykneescan.com	Within 5 working days
General complaint (including data matters)	info@mykneescan.com	Acknowledged within 3 working days; resolved within 20
Urgent data security concern	info@mykneescan.com (marked URGENT)	Same working day

If you are not satisfied with our response, you have the right to lodge a complaint with the Information Commissioner's Office (ICO), the UK's independent data protection regulator:

ICO Contact	Detail
Website	www.ico.org.uk
Helpline	0303 123 1113
Postal address	Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Online complaint form	ico.org.uk/make-a-complaint

17. Under-18s — Exclusion from Self-Referral Services

MyKneeScan's self-referral booking and clinical vetting services are available to adults aged 18 and over only. We do not knowingly collect personal data from individuals under the age of 18 through this platform.

If we become aware that personal data has been collected from a person under the age of 18 without appropriate authorisation, we will:

- Cancel the booking and issue a full refund
- Delete the data promptly
- Notify the parent or guardian where appropriate

Patients under 18 who require private knee imaging should be referred through their GP or paediatric orthopaedic pathways. MyKneeScan does not operate a paediatric service.

If you are a clinician or parent seeking imaging for a patient or child under 18, please contact info@mykneescan.com to discuss appropriate referral pathways.

18. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our processing activities, legal requirements, or ICO guidance. The current version is always available at www.mykneescan.com/privacy.

Where changes are material — for example, where we add a new purpose for processing health data, change a lawful basis, or add a new category of data recipient — we will notify existing registered users by email at least 14 days before the change takes effect and will seek fresh consent where required.

Version history is maintained and available on request from info@mykneescan.com.

19. Contact Details

Role / Contact Type	Detail
Data controller	MyKneeScan Ltd (subsidiary of SportsHealing Holdings)
Registered office	Woodlands Grange, Woodlands Lane, Bradley Stoke, Bristol, England, BS32 4JY
Privacy and data protection	info@mykneescan.com
General enquiries and complaints	info@mykneescan.com
Clinical governance queries	info@mykneescan.com
Urgent data security	info@mykneescan.com (marked URGENT in subject line)
Telephone	020 7483 5160
ICO registration number	ZB123456
Website	www.mykneescan.com/privacy

Appendix A — Key Service Providers (Data Processors)

The following processors handle personal data on MyKneeScan's behalf under Data Processing Agreements. This list will be updated when suppliers change; the current version is always available at www.mykneescan.com/privacy.

Supplier / Role	Data Processed	Location	Transfer Safeguard
Semble Patient management and booking database	Identity, contact, booking records, health data	UK	N/A — UK based
Google Cloud Platform Hosting and infrastructure	All platform data (stored in UK region only — eu-west-2 London)	UK (London region)	TRA completed; US-ownership risk assessed as low given UK-only storage
Payment provider [Stripe / Square — to be confirmed]	Payment tokens and transaction references only (not card data)	UK/EEA	IDTA or adequacy — to be confirmed on provider selection
Email and SMS provider [to be confirmed]	Contact details for appointment communications	UK/EEA preferred	To be confirmed on provider selection
Analytics provider [GA4 or equivalent — where consented]	Pseudonymised website usage data (consented users only)	UK/EEA	To be confirmed; ICO guidance on GA4 to be applied

Note: Placeholder entries marked [to be confirmed] must be completed before go-live.

Appendix B — Cookie Categories

Category	Examples	Consent Required	Can Be Disabled?
Strictly necessary	Session ID, CSRF tokens, booking flow state, login authentication	No — essential for service operation	No
Functional	Saved preferences, remembered location, accessibility settings	Yes — opt-in required	Yes — via cookie settings
Analytics	Page view tracking, user journey analysis, performance monitoring (anonymised/pseudonymised)	Yes — opt-in required under UK PECR	Yes — via cookie settings
Marketing	Conversion tracking for opted-in users only. No health-data-based targeting.	Yes — explicit opt-in only	Yes — via cookie settings or unsubscribe

Appendix C — Version History

Version	Effective Date	Key Changes
v1.0	[Original date]	Initial policy — described MyKneeScan as a direct clinical provider. Vague retention periods. Limited Article 9 basis. No breach notification section. Placeholders unresolved.
v2.0	1 May 2026	Full redraft. Accurate marketplace/broker model description. Controller vs processor distinction added. Specific retention schedule. Strengthened Art. 9 basis with explicit consent. Clinical Advisory Panel added as data recipient. Data breach notification section added (Section 15). Under-18s explicitly excluded (Section 17). ICO contact details added. DPO appointed. GCP transfer risk assessment noted. Cross-reference to Scan Vetting Pro Forma MKS-VF-001 added. Complaints email confirmed as info@mykneescan.com.