



# Privacy Policy

**Dr. K Parmar, Registered Manager, Elite Sports Professional Services**

**Version Control:**

- **Version 1:** April 2024 by Dr. K Parmar
- **Version 2:** August 2024 by Dr. K Parmar
- **Review date:** August 25 by Dr K Parmar, Registered manager

---

## Introduction

At Elite Sports Professional Services Limited ("ESPS"), we are committed to protecting and respecting your privacy. This Privacy Policy explains how we collect, use, and safeguard the personal data that we obtain from you, and how we comply with the General Data Protection Regulation (GDPR). We understand the importance of your privacy, especially when it comes to sensitive healthcare data, and we are dedicated to ensuring that your personal information is handled with the utmost care and security.

## Contact Information

### Elite Sports Professional Services Limited

Eight Members Club  
One Dysart Street  
London EC2A 2BX

For any queries related to this Privacy Policy or your personal data, you can contact our Data Protection Officer via:

- **Email:** [parmar.admin@lips.org.uk](mailto:parmar.admin@lips.org.uk)
- **Phone:** +44 20 7392 9410
- **Postal Address:** Eight Members Club, One Dysart Street, London EC2A 2BX

We contract our services through **London International Patient Services Limited** ("LIPS"), which handles our administration and ensures our compliance with GDPR.

## 1. Who We Are

When we refer to "we," "us," or "our," we are referring to **Elite Sports Professional Services Limited**. When we refer to "LIPS," "they," or "their," we are referring to **London International Patient Services Limited**.

LIPS is a private limited company registered in England and Wales. In most instances, LIPS is the "Data Controller" of your personal data. As the Data Controller, LIPS is responsible for deciding how your personal data is processed, ensuring it is secure, and that any third parties we collaborate with also follow strict data protection standards.

In rare instances where another organization or individual acts as the Data Controller, we will inform you of this arrangement and provide the necessary contact details.

## 2. What We Do with Your Personal Data

We collect and process personal data to support our healthcare services and to fulfill our contractual obligations. The data we collect may include your medical history, contact details, and other relevant information necessary to provide you with the highest standard of care.

We also process your data for administrative purposes, including billing, compliance with legal obligations, and, in some cases, for marketing and communications if you have given us your explicit consent.





### 3. What Personal Data Do We Collect?

The personal data we collect from you varies depending on your interaction with our services. Here is a detailed breakdown of the data we collect:

- **Website Visitors:** When you visit our website, no personal data is required. However, your browser automatically transmits data such as your IP address, browser type and settings, operating system, and the date and time of your visit.
- **Service Users:** If you register for our services, we collect the following data, handled through LIPS:
  - Name
  - Patient Number
  - Contact Information (Phone, Email)
  - GP Name and Address
  - Health Insurance Information
  - Financial Details
  - Confidential Correspondence
  - Digital Images and Photographs
  - Medical Reports, Blood Test Results, Treatment Results
  - Clinical Treatment Records
  - Results of Assessments

The legal bases for processing this data include explicit consent from you, the necessity of processing for medical diagnosis, and compliance with our contractual obligations.

### 4. How Do We Protect Your Personal Data?

We take the protection of your personal data seriously and implement a range of measures to ensure its safety:

- **Data Minimization:** We collect only the data necessary for the purpose at hand and retain it only as long as required by law or our legitimate business needs.
- **Security Controls:** We employ physical, technical, and procedural safeguards to protect your data from unauthorized access, loss, or destruction. These include:
  - Physical security controls at our offices and data storage facilities.
  - IT controls, such as access restrictions, encryption, and intrusion detection systems.
  - Contractual agreements with third-party providers to ensure they comply with our data protection standards.

### 5. Your Rights Under GDPR

Under GDPR, you have several rights concerning your personal data, including:

- **Right to Access:** You can request access to the personal data we hold about you. We will provide you with a copy of your data unless there are legal or confidentiality reasons that prevent us from doing so.
- **Right to Rectification:** If your data is incorrect, you can request that we correct it.
- **Right to Erasure:** You can request the deletion of your data under certain conditions.
- **Right to Restrict Processing:** You can request that we restrict the processing of your data in certain situations.



- **Right to Data Portability:** You can request that we transfer your data to another service provider.
- **Right to Withdraw Consent:** If we are processing your data based on your consent, you have the right to withdraw that consent at any time.

## **6. How We Lawfully Process Your Data**

We process your data on several legal bases:

- **Contractual Necessity:** Processing is necessary for us to provide the services you have requested, including medical care and treatment.
- **Legal Obligations:** We may process your data to comply with legal obligations, such as reporting to health authorities or regulatory bodies.
- **Legitimate Interests:** We may process your data to improve our services, ensure safety and quality, and for administrative purposes, as long as it does not infringe on your rights and freedoms.
- **Explicit Consent:** In some cases, such as marketing communications or participation in clinical research, we will only process your data if we have your explicit consent.

## **7. Sources of Data Collection**

We primarily collect data directly from you, your Consultant, or referring bodies. In some cases, we may receive your data from third parties such as your GP, insurance companies, or embassies, but you will typically be aware of this transfer of data.

## **8. Who We Share Your Data With**

While we aim to minimize data sharing, there are instances where sharing your data with third parties is necessary:

- **Consultants and Healthcare Providers:** To provide you with the best care possible.
- **Service Providers:** Such as IT support, medical equipment suppliers, or payment processors.
- **Regulatory Bodies:** Such as the Care Quality Commission (CQC) or General Medical Council (GMC), when required.
- **Legal and Financial Advisors:** For handling disputes, insurance claims, or legal obligations.
- **Debt Collection Agencies:** For the collection of unpaid bills.
- **International Transfers:** If your care involves providers or facilities outside the UK, we may need to share your data internationally, always ensuring that appropriate safeguards are in place.

## **9. Data Storage and International Transfers**

Your data may be stored in both physical and cloud-based systems, some of which may be located outside the UK or EEA. When we transfer your data internationally, we ensure it is protected according to GDPR requirements, using contracts and technical safeguards.

## **10. Data Retention**



We retain your personal data only for as long as necessary to fulfill the purposes for which it was collected or to comply with legal, regulatory, or business requirements. Factors that influence our retention periods include:

- **Legal Obligations:** Data retention periods required by law.
- **Business Needs:** For example, records needed for medical history or ongoing treatment.
- **Risk Assessment:** Considering the sensitivity of the data and the potential risk of harm from unauthorized use or disclosure.

## **11. How We Protect Your Data**

We are committed to ensuring the security of your data through various means:

- **Organizational Standards:** Company-wide policies and procedures for data protection.
- **Technical Security:** IT controls to prevent unauthorized access.
- **Physical Security:** Secure premises and restricted access.
- **Training and Awareness:** Regular staff training on data protection and security.
- **Specialist Roles:** Dedicated Data Protection Officers and Information Governance teams to oversee data security.

## **Your Rights Under GDPR**

You have the following rights regarding your personal data:

- **Right to Be Informed:** Know how your data is being used.
- **Right to Access:** View the data we hold about you.
- **Right to Rectification:** Correct any inaccuracies.
- **Right to Erasure:** Request deletion of your data.
- **Right to Restrict Processing:** Limit how we use your data.
- **Right to Data Portability:** Transfer your data to another provider.
- **Right to Object:** Oppose certain uses of your data.
- **Rights Related to Automated Decision-Making:** Including profiling.

## **Compliance and Security**

We use Comupcare, a web-based clinical management application developed by Streets Heaver, to ensure GDPR compliance and secure patient records.



- **Physical Security:** Data is stored in secure, geographically dispersed UK data centres with biometric and key-pass access controls.
- **Technical Security:** Access to Compucare is secured by multiple layers of protection, including firewalls, intrusion detection, and two-factor authentication.
- 
- **Procedural Security:** Access is restricted to authorized personnel, and all activities are monitored for unusual access patterns.

### **Data Controllers and Data Processors**

Under GDPR, Compucare acts as a Data Processor on behalf of **LIPS**, who are the Data Controllers. COMPUCARE processes personal data only as instructed by LIPS.

How you can find out more information If you have any questions or queries about how we handle your personal data at LIPS, please get in touch at [dataprotection@lips.org.uk](mailto:dataprotection@lips.org.uk)

London International Patient Services (LIPS) takes your privacy and information security seriously. The UK and EU General Data Protection Regulation (GDPR) came into force on the 25th of May 2018. The GDPR changes how personal data is handled and increases or reinforces the rights of data subjects.

LIPS have appointed IT Governance Europe Limited to act as our EU representative. If you wish to exercise your rights under the EU General Data Protection Regulation (EU GDPR), or have any queries in relation to your rights or general privacy matters, please email our Representative at [eurep@itgovernance.eu](mailto:eurep@itgovernance.eu) Our Data Protection Officer (DPO) is GRCI Law Limited, Unit 3, Clive Court, Bartholemew's Way, Cambridgeshire Business Park, Ely CB7 4EA. Please ensure to include our company name in any correspondence you send to our Representatives.